

FIG. 1

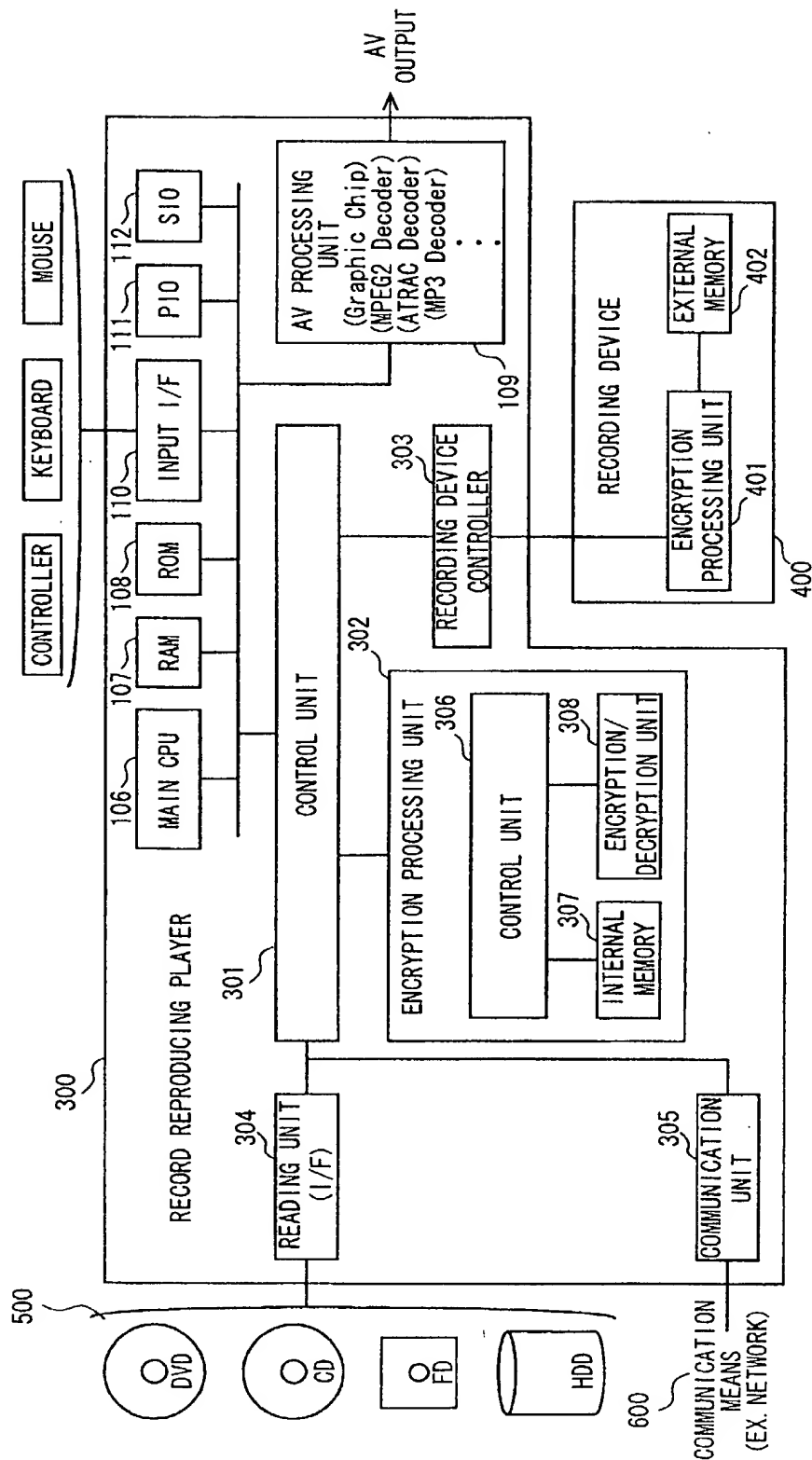


FIG. 2

FIG. 3

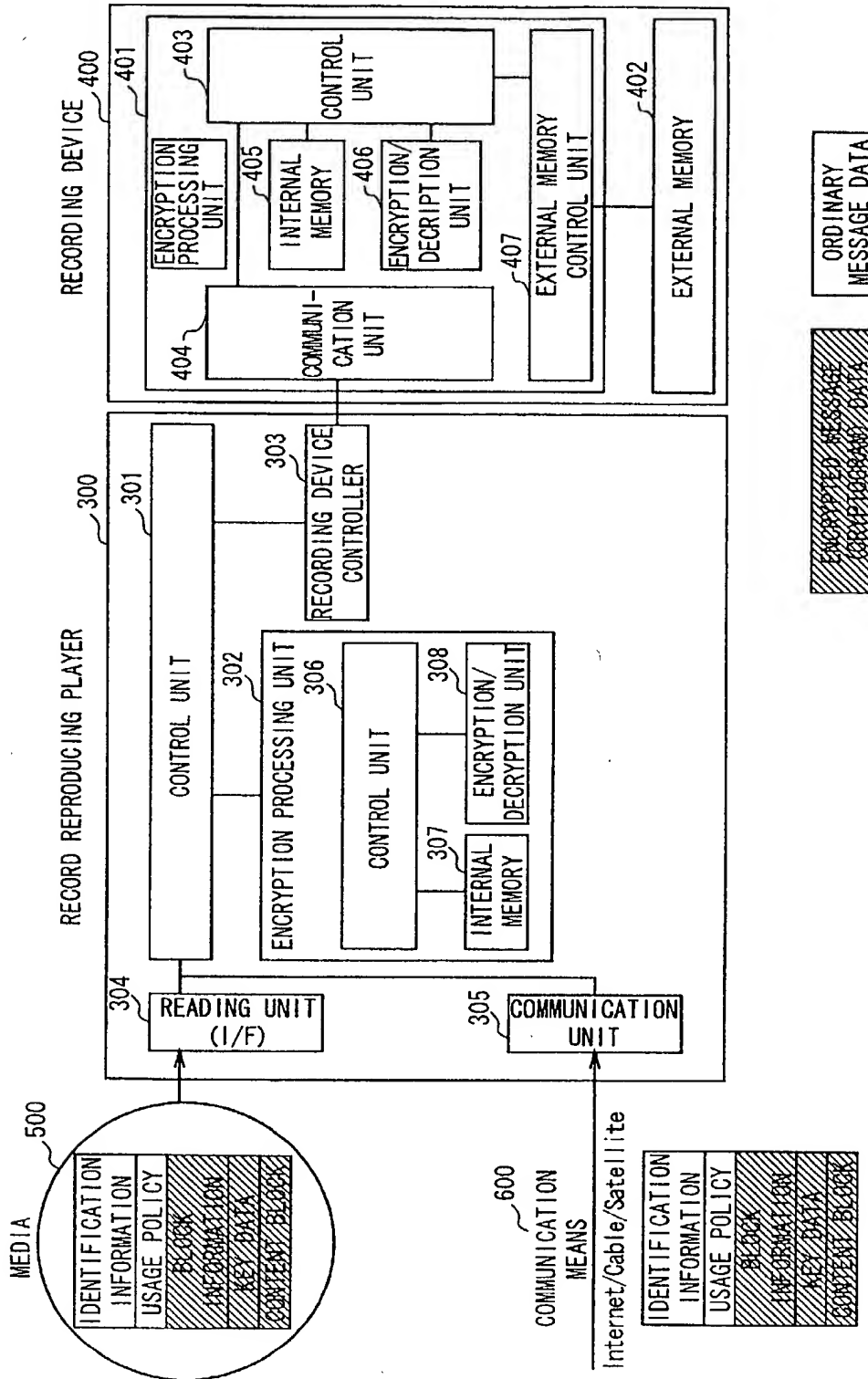
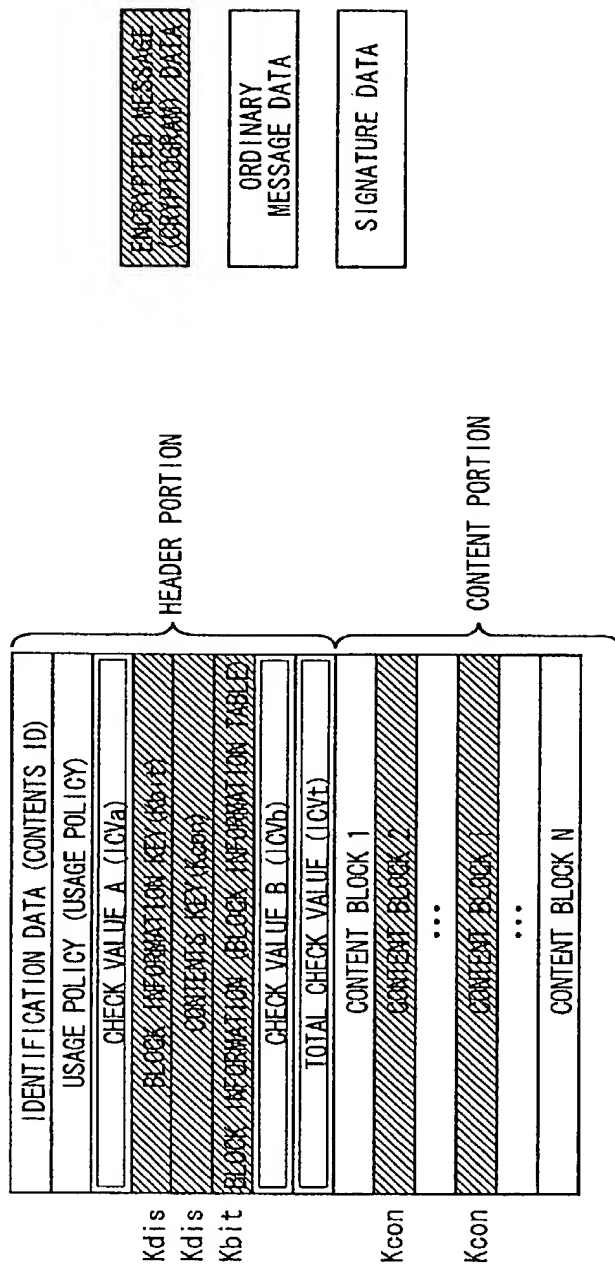


FIG. 3



DATA FORMAT ON MEDIA & COMMUNICATIONS ROUTE

FIG. 4

HEADER LENGTH
CONTENT LENGTH
FORMAT VERSION
FORMAT TYPE
CONTENT TYPE
OPERATION PRIORITY
LOCALIZATION FIELD
COPY PERMISSION
MOVE PERMISSION
ENCRYPTION ALGORITHM
ENCRYPTION MODE
INTEGRITY CHECK METHOD

USAGE POLICY

FIG. 5

09937410-121701

09/937410

09/937410

09/937410

Kbit	BLOCK 1	BLOCK NUMBER
		BLOCK LENGTH
		ENCRYPTION FLAG
		ICV FLAG
		ICV1
		.
		.
		.
		.
		.
BLOCK N	BLOCK LENGTH	
	ENCRYPTION FLAG	
	ICV FLAG	
	ICVN	

BLOCK INFORMATION

FIG. 6

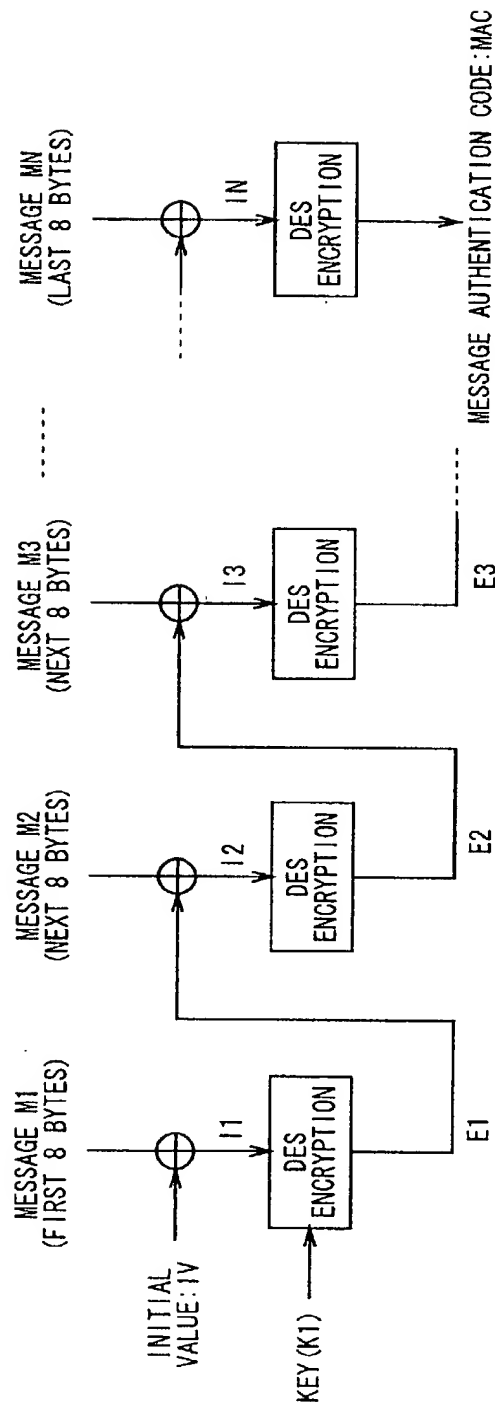


FIG. 7

TOTAL 0442E660

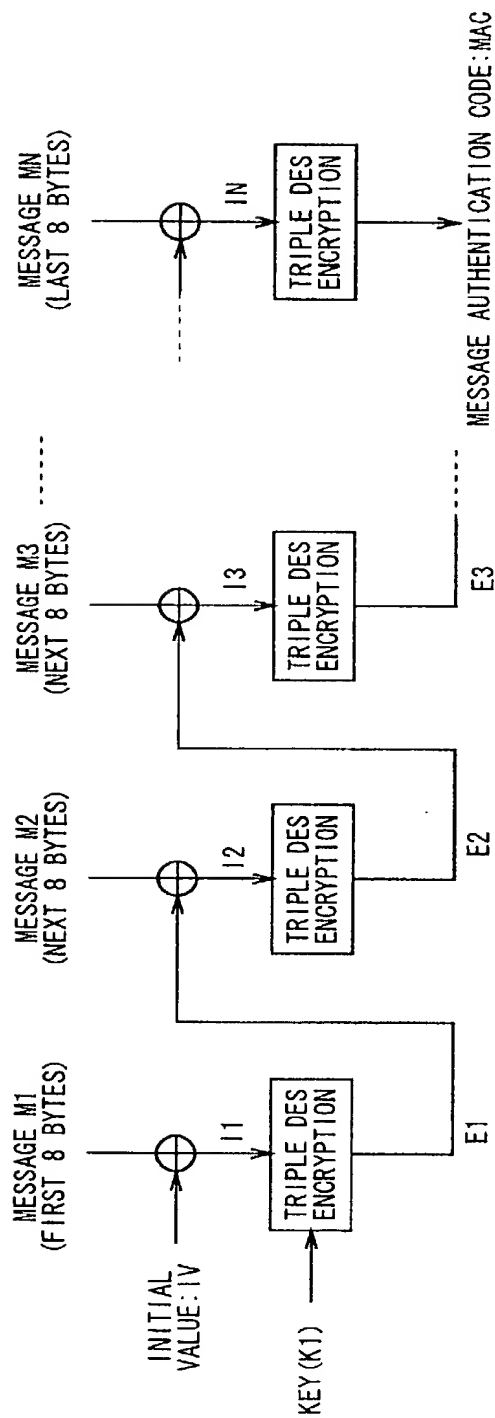


FIG. 8

FOUO-014660

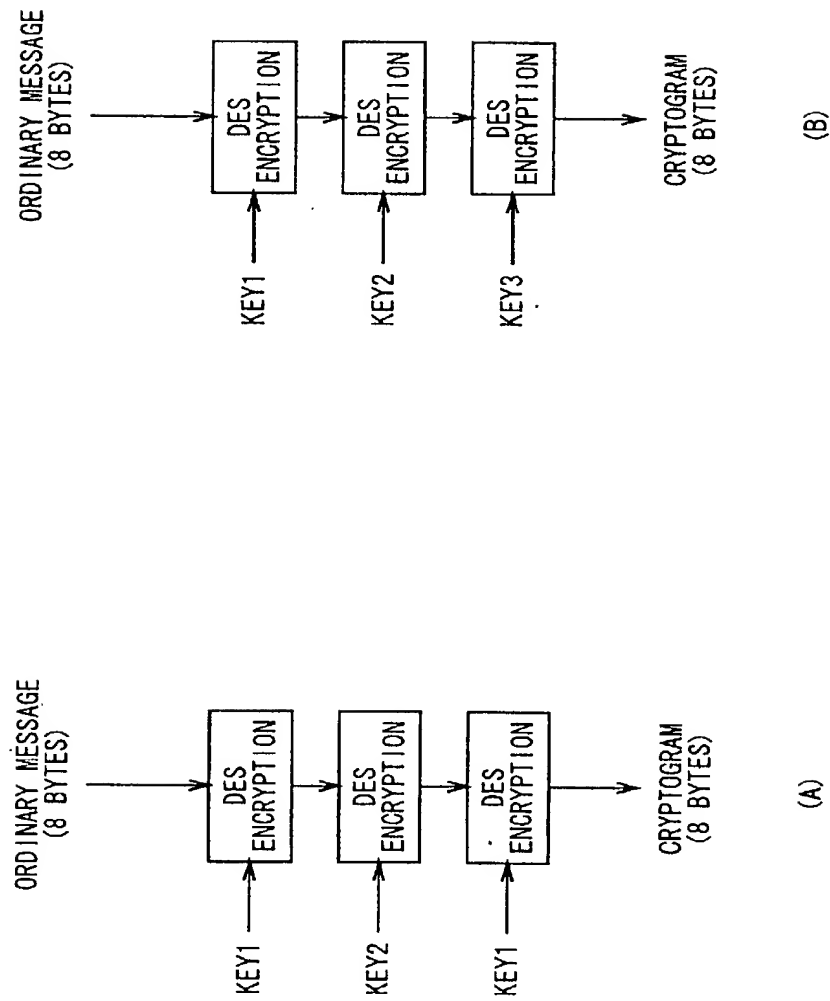


FIG. 9

TOTAL: 0442660

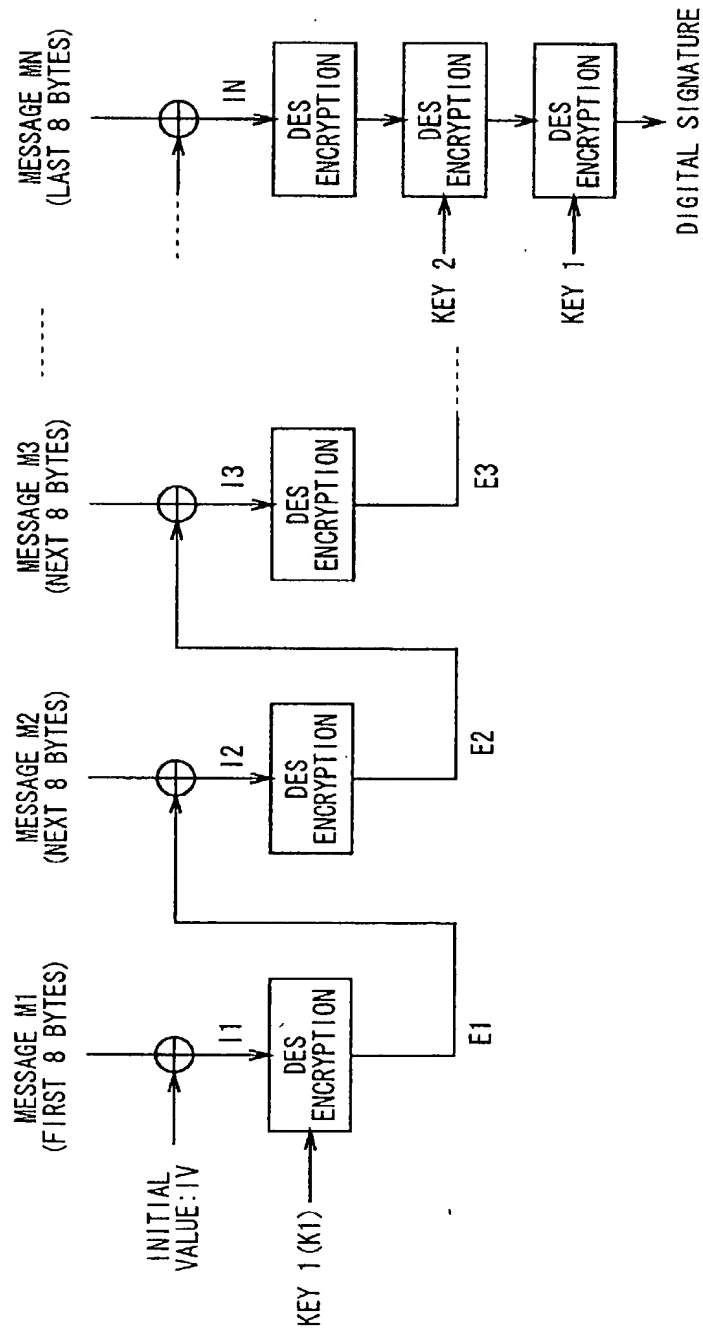
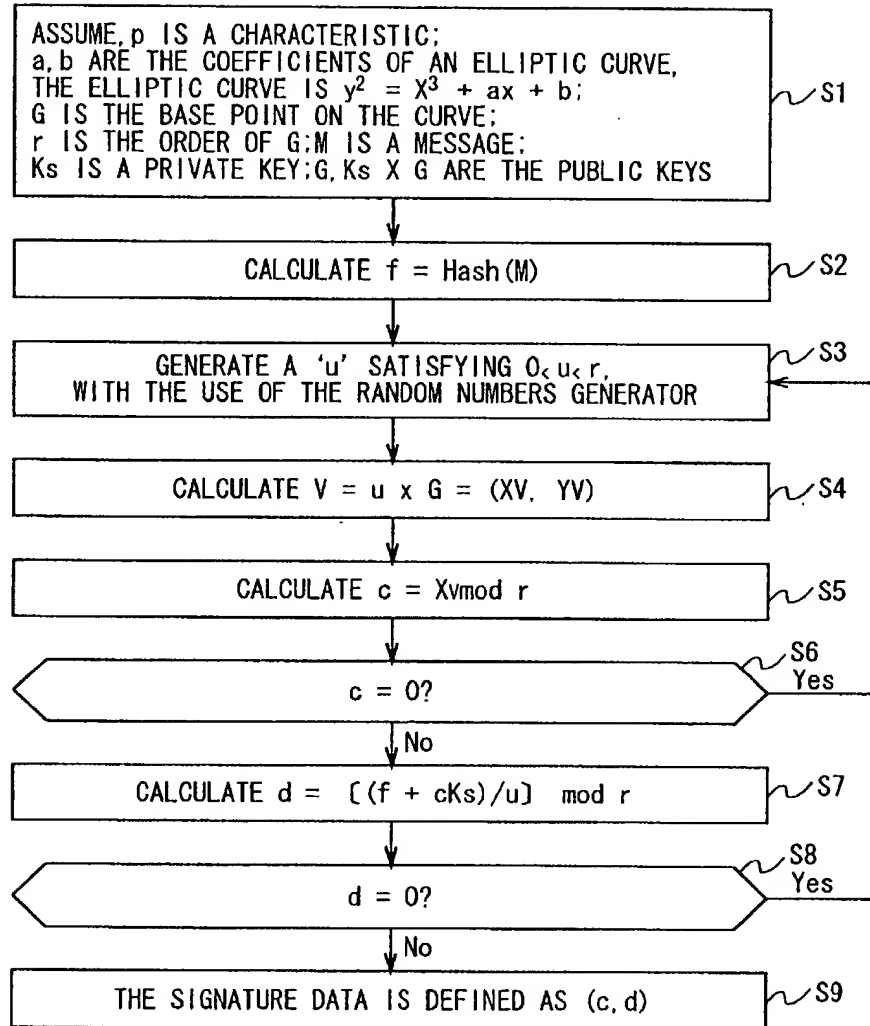


FIG. 10

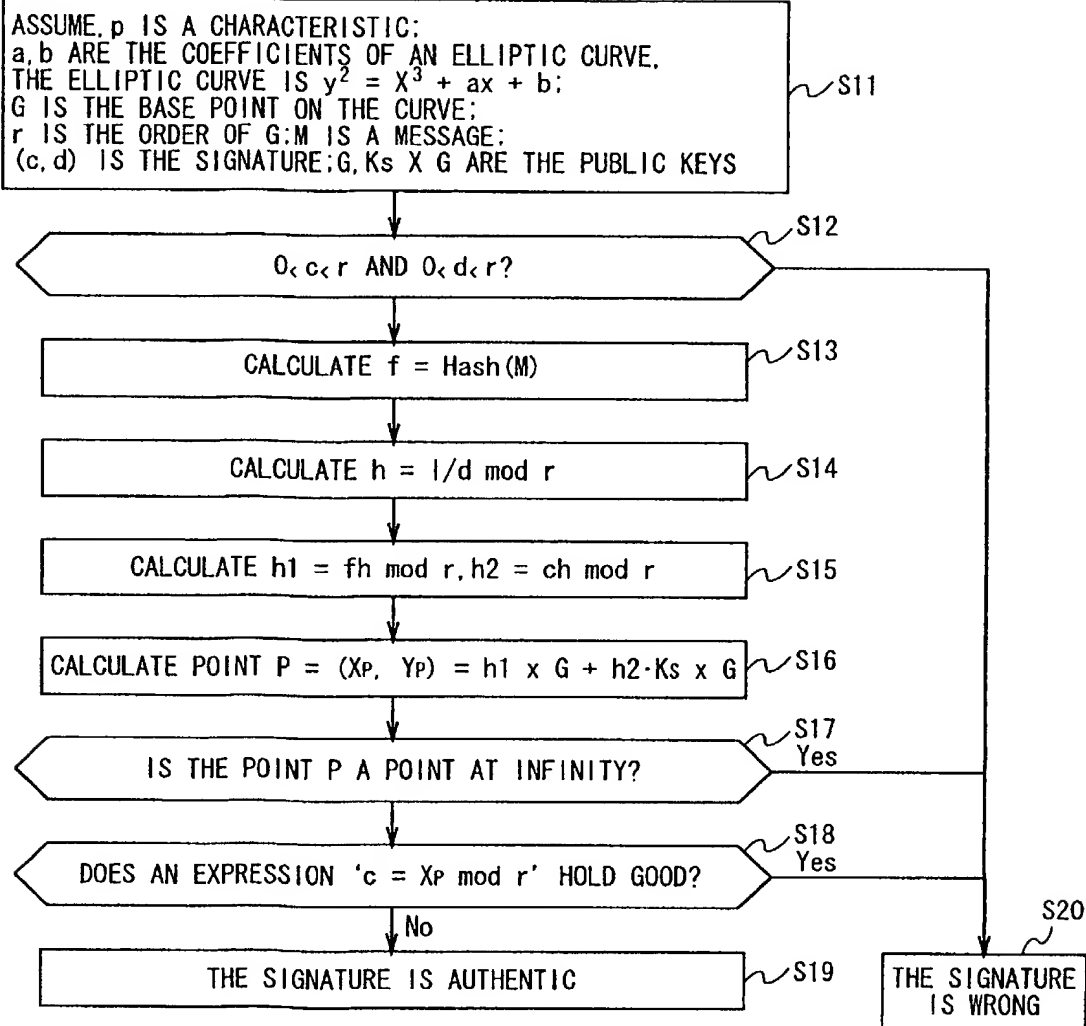
# GENERATION OF SIGNATURE



GENERATION OF SIGNATURE (IEEE P1363/D3)

FIG. 11

## AUTHENTICATION OF SIGNATURE



AUTHENTICATION OF SIGNATURE (IEEE P1363/D3)

FIG. 12

12/93

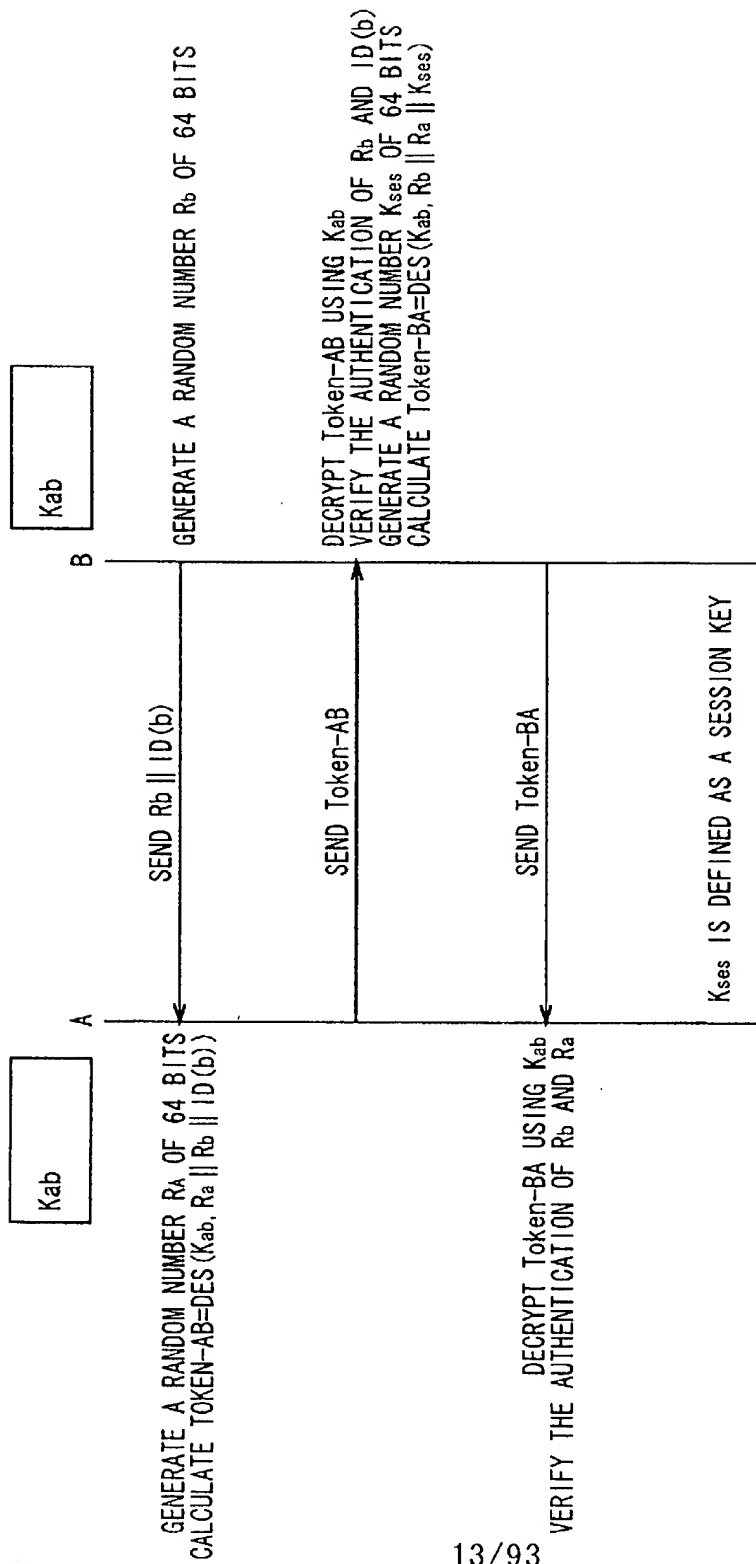


FIG. 13

ISO/IEC 9798-2 MUTUAL AUTHENTICATION AND SHARED KEY DEVICE USING SYMMETRIC ENCRYPTION TECHNOLOGY

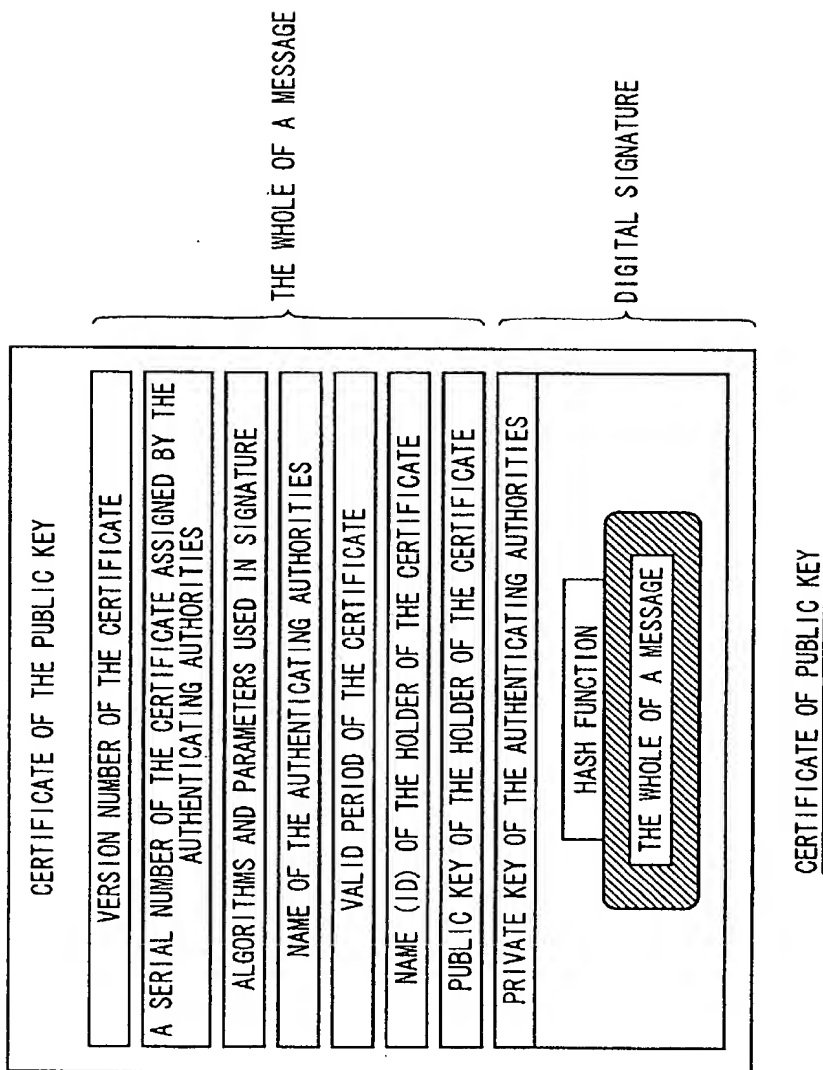
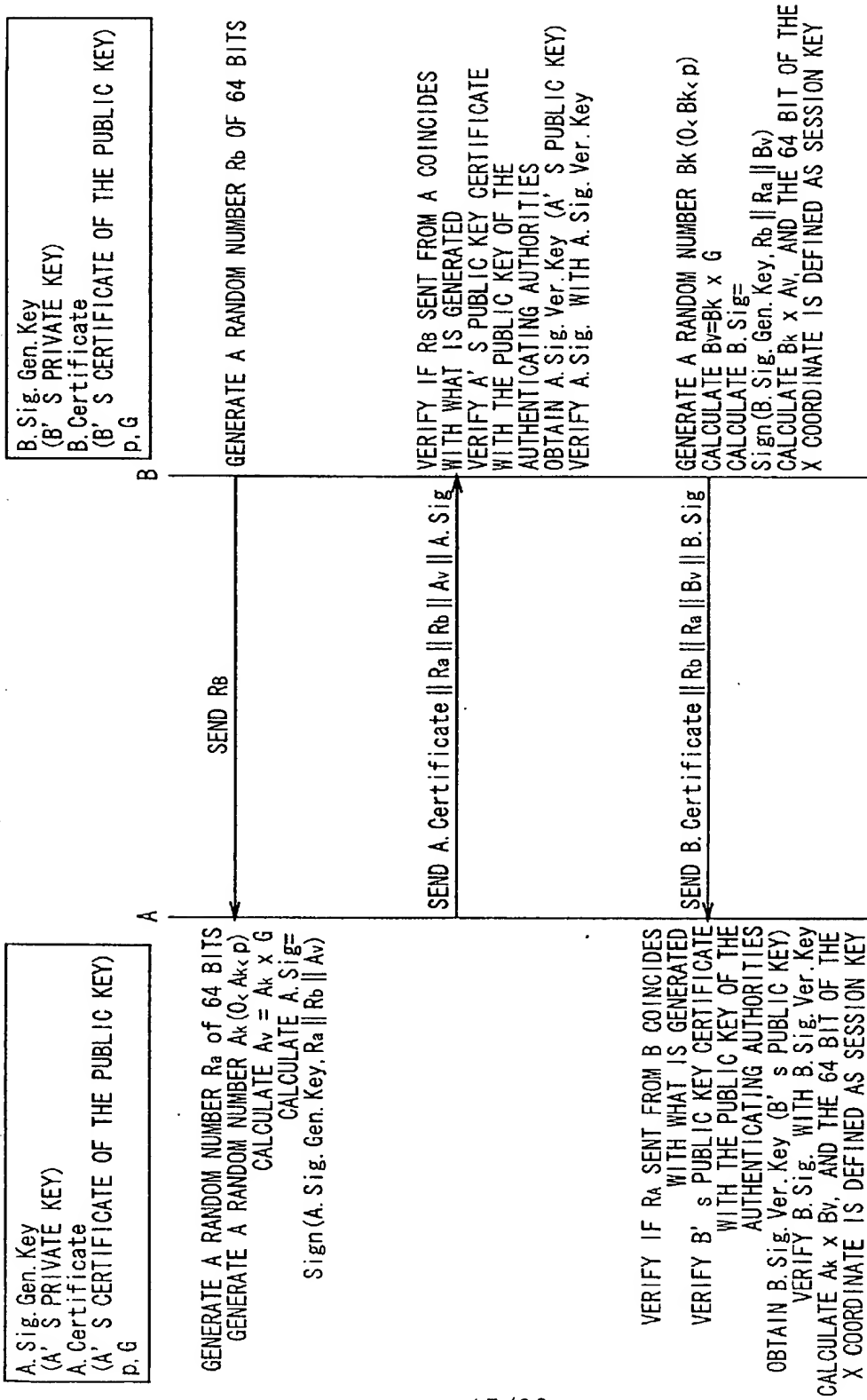


FIG. 14

FOUO 0142660



ISO/IEC 9798-3 MUTUAL AUTHENTICATION AND SHARED KEY SYSTEM USING SYMMETRIC  
ENCIPHERMENT ALGORITHMS (SYMMETRIC KEY ENCRYPTION TECHNOLOGY)

FIG. 15

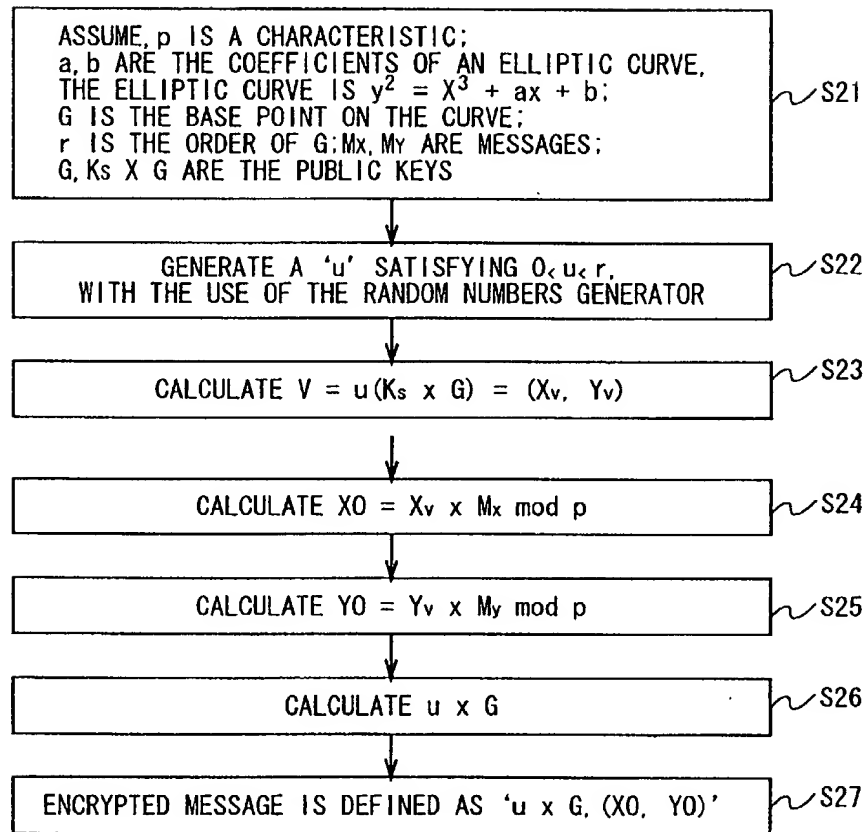
ENCRYPTIONENCRYPTION USING ELLIPTIC CURVE ENCRYPTION METHOD (MENEZES-VANSTONE)

FIG. 16

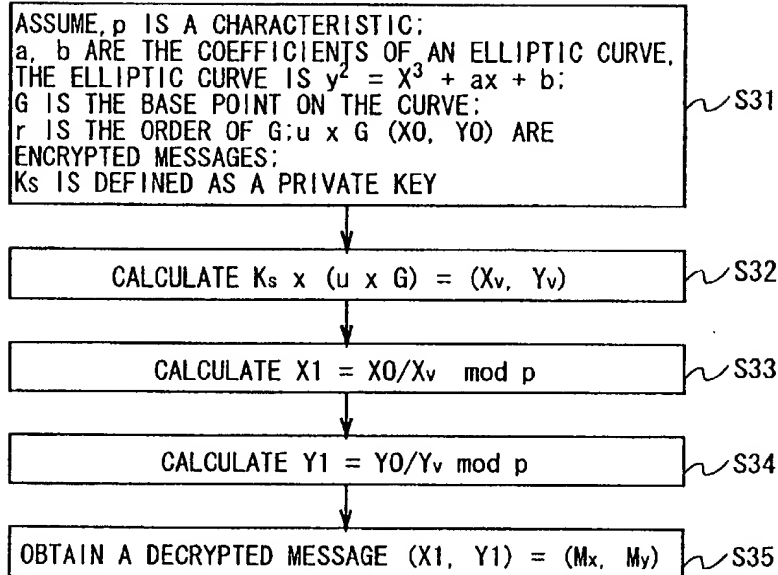
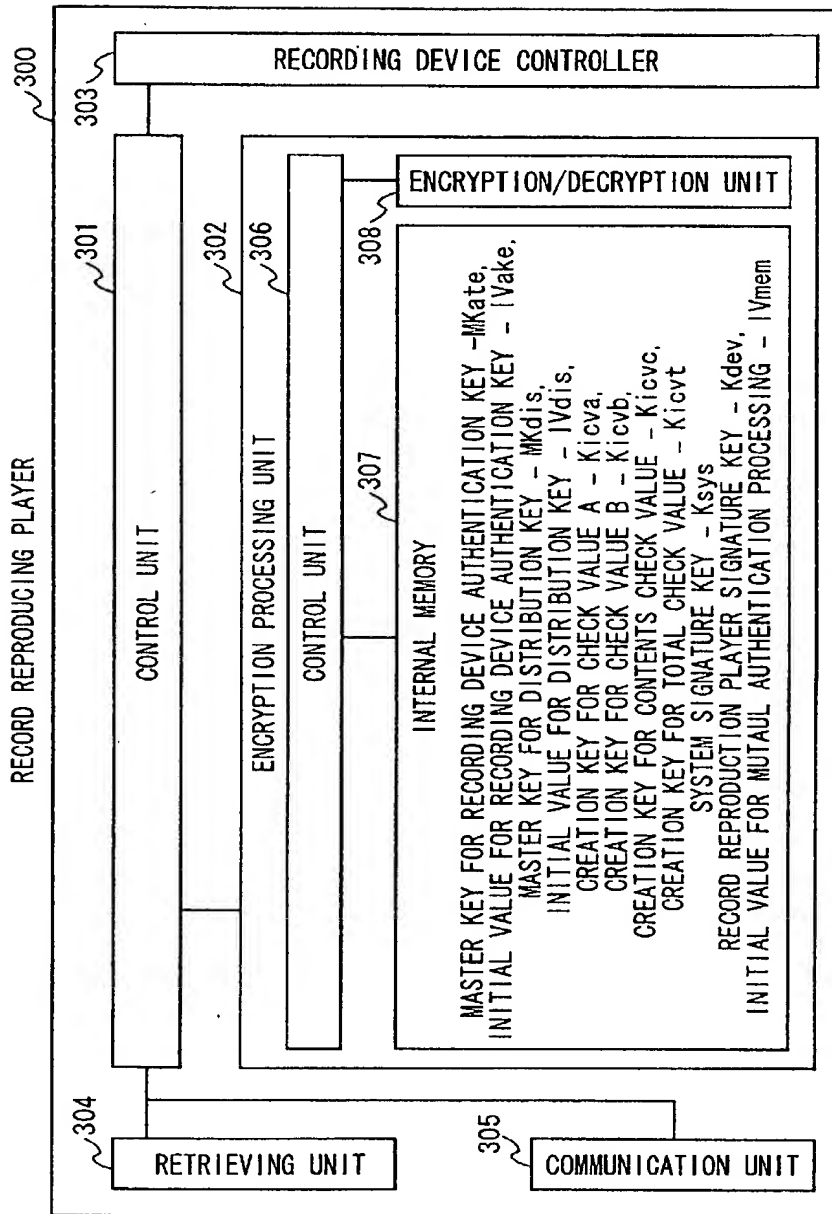
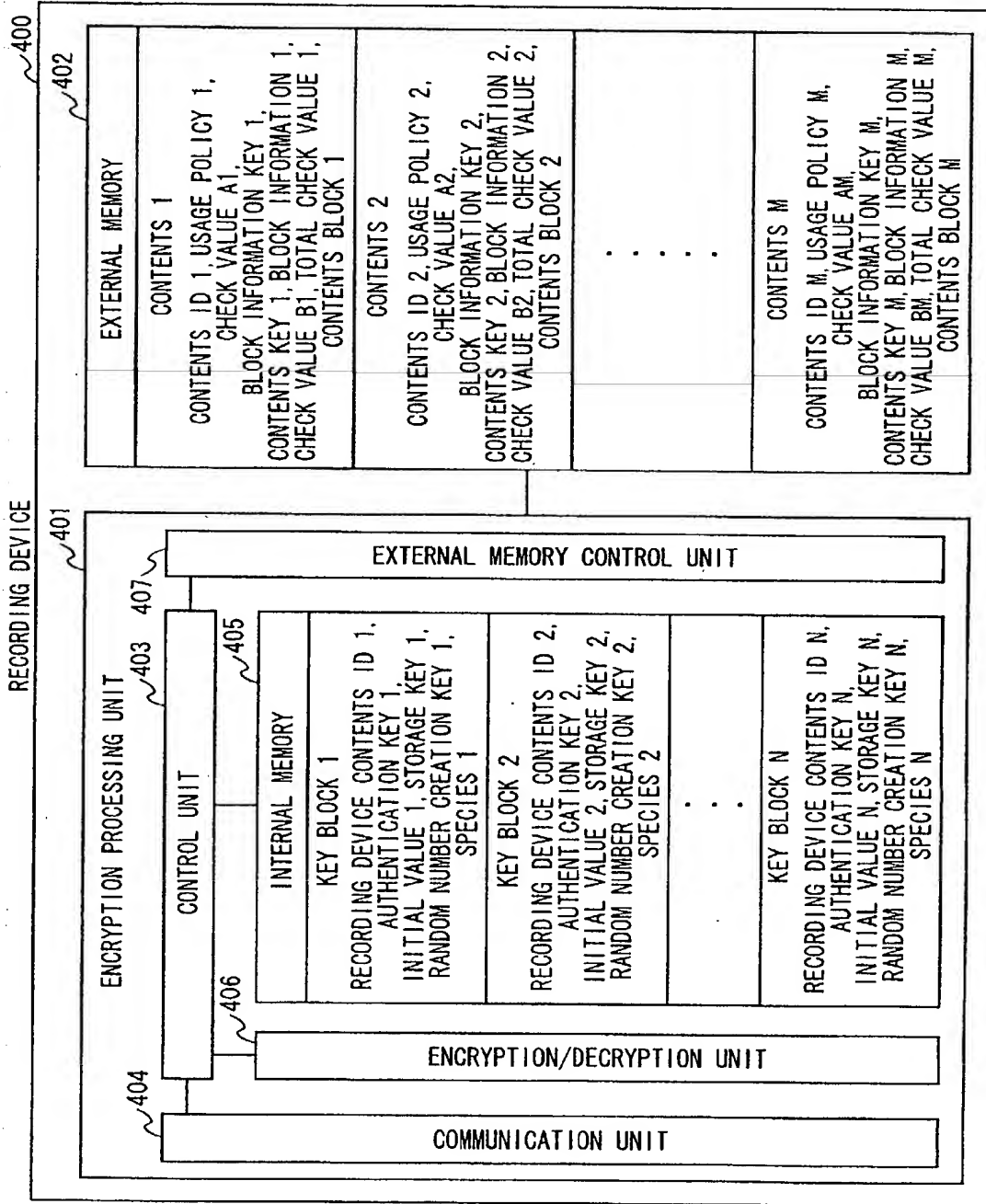
DECRYPTIONDECRYPTION USING ELLIPTIC CURVE ENCRYPTION MTHOD (MENEZES-VANSTONE)

FIG. 17

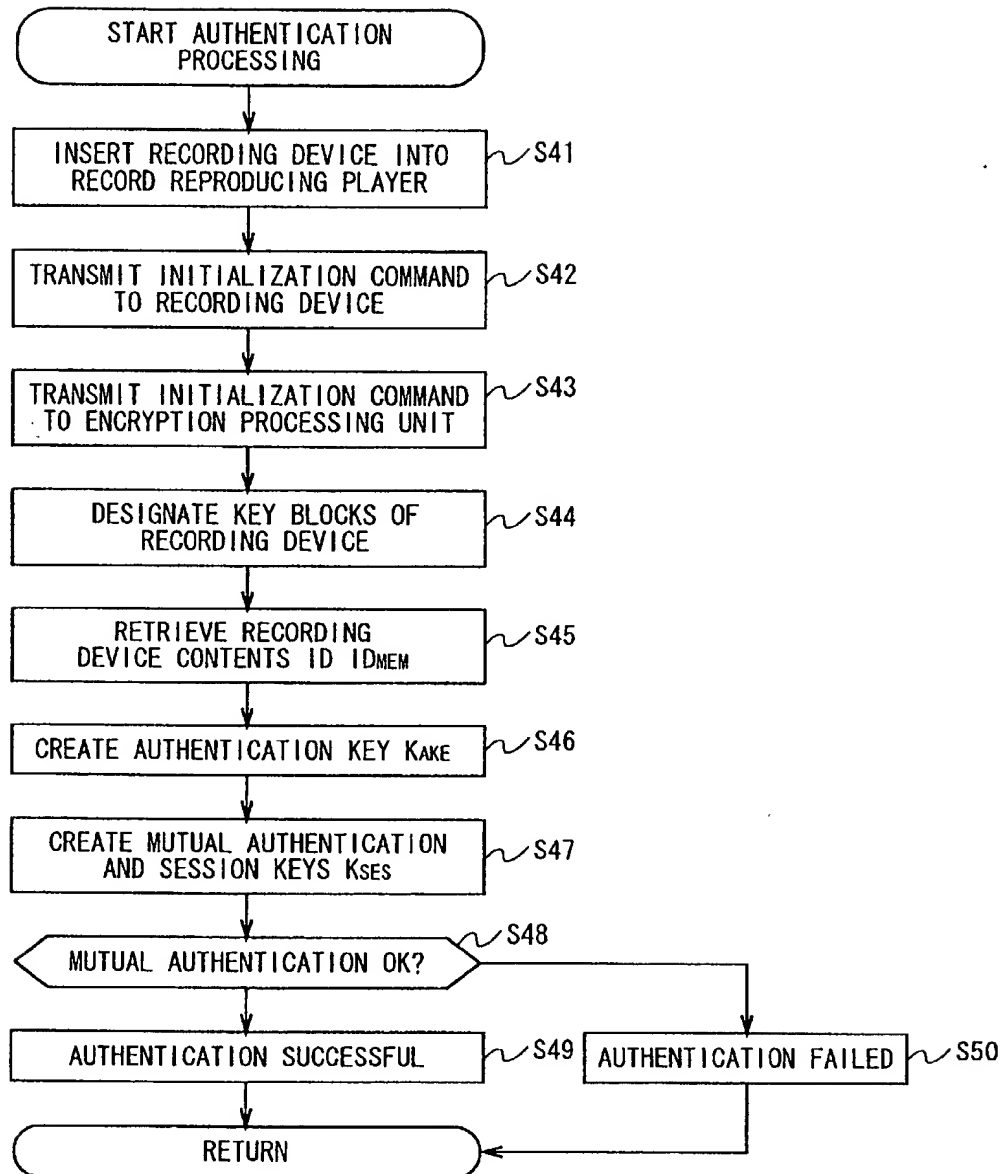


DATA RETAINING STATE ON RECORD REPRODUCING PLAYER

FIG. 18



DATA RETAINING STATE ON RECORDING DEVICE FIG. 19



MUTUAL AUTHENTICATION BETWEEN RECORD REPRODUCTION AND RECORDING DEVICE

FIG. 20

FOOTNOTES

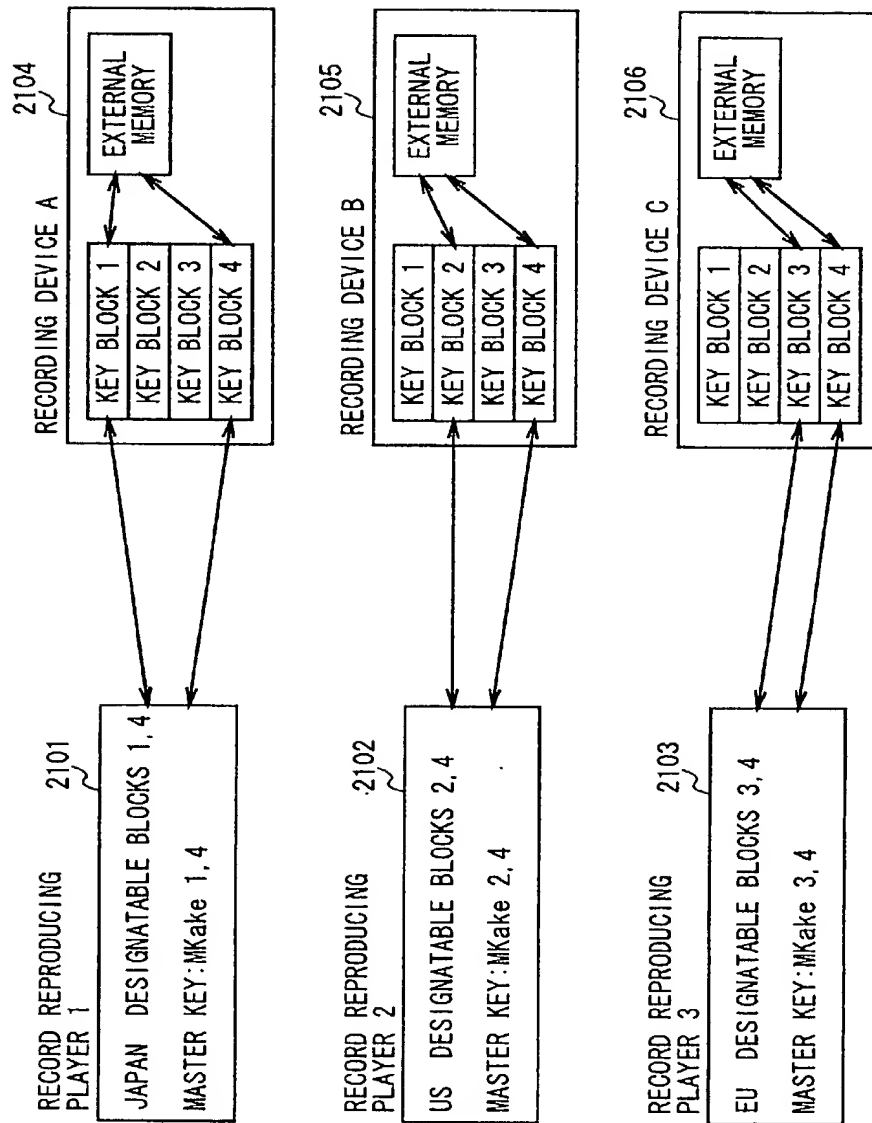


FIG. 21

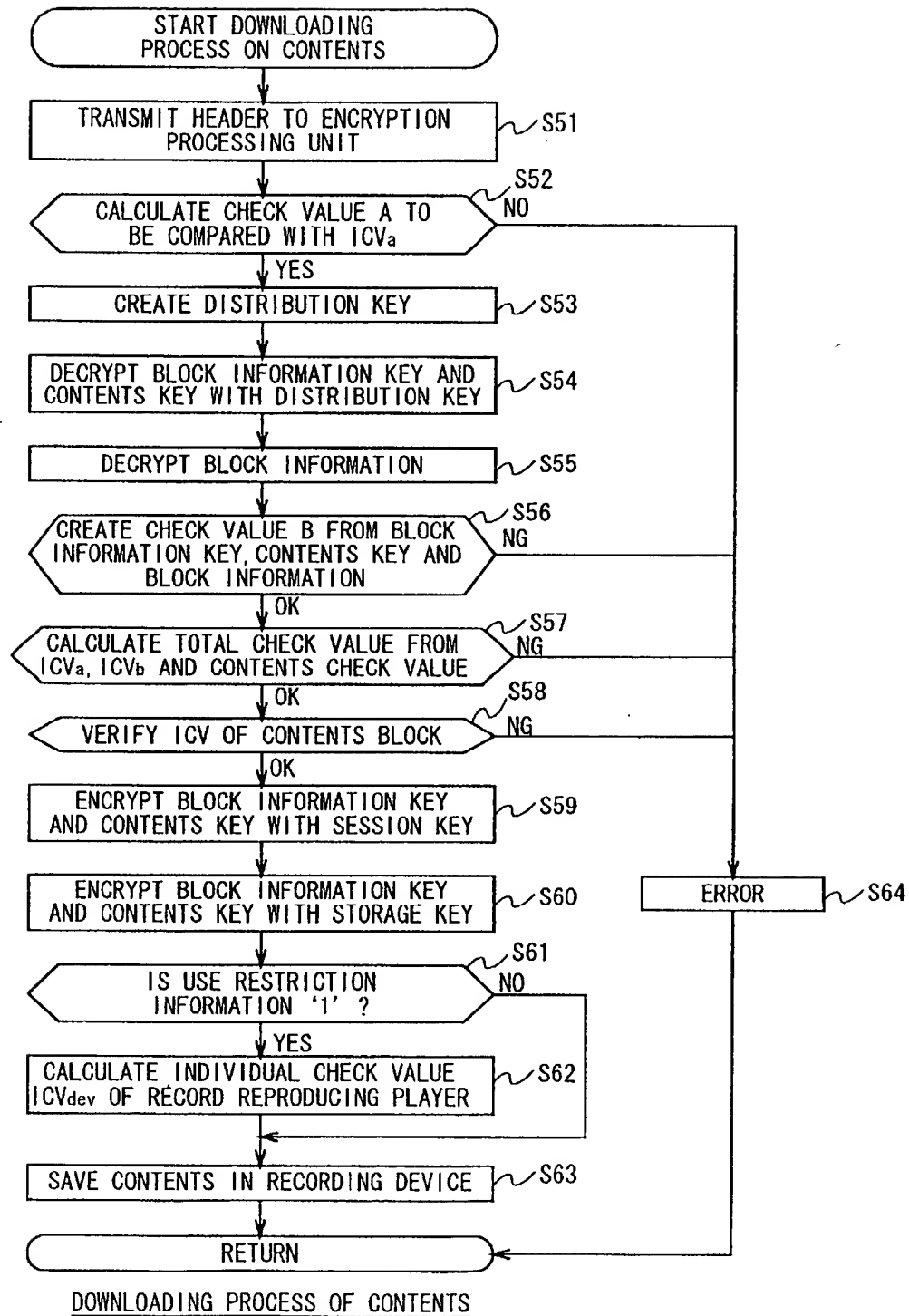
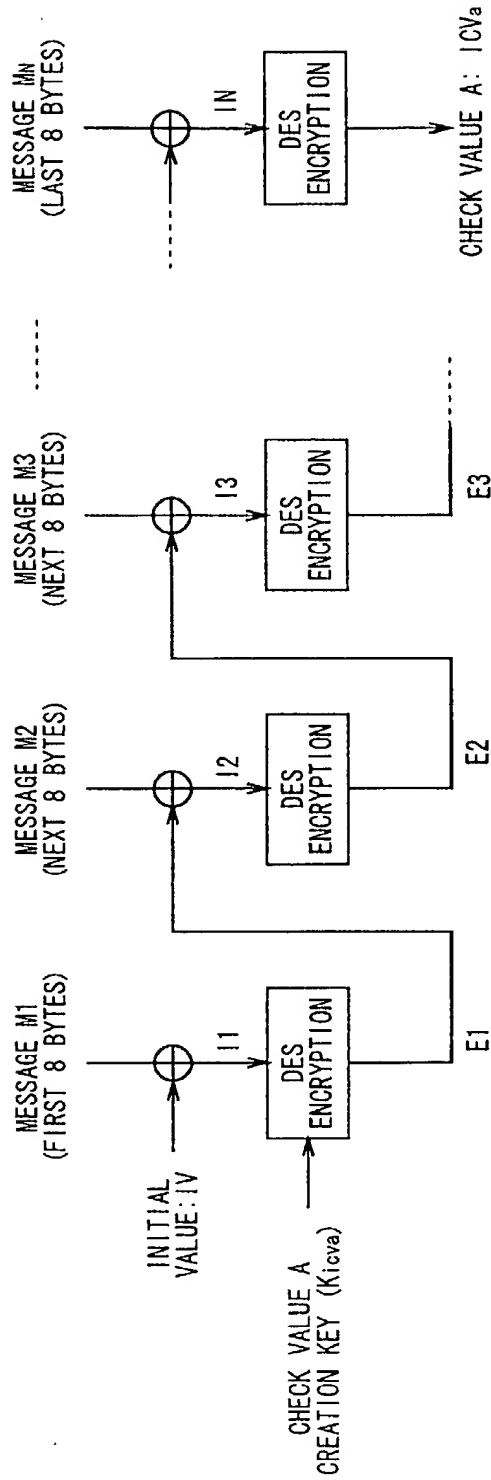
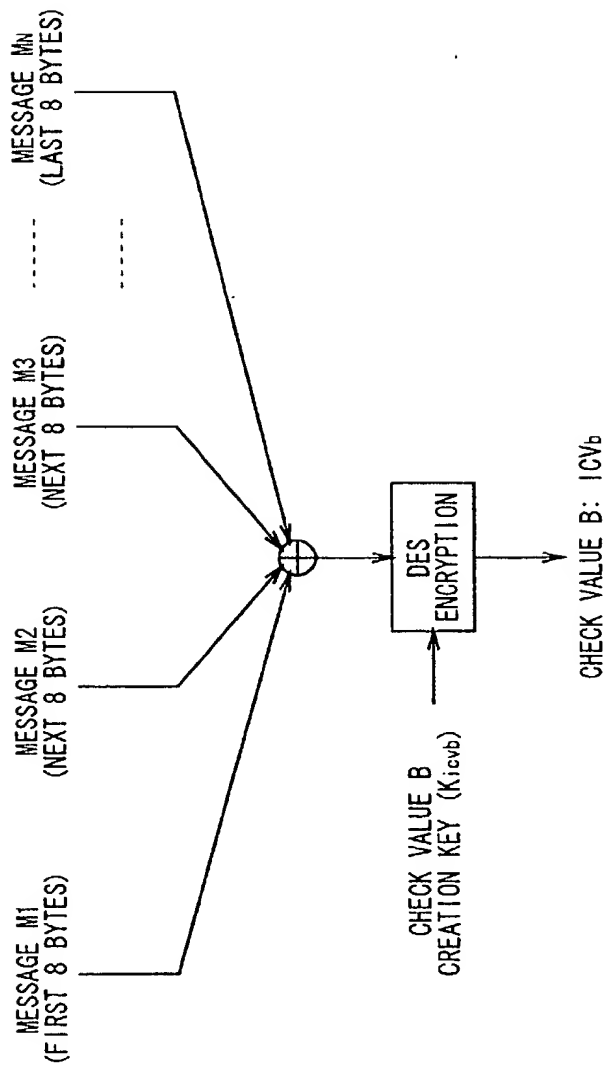


FIG. 22



MESSAGE M1 - MN: CONTENTS ID, USAGE POLICY  
 $\oplus$ : EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 23



MESSAGE M1 - MN: BLOCK INFORMATION KEY  $K_{bit}$ , CONTENTS KEY  $K_{con}$ , BLOCK INFORMATION  
 $\oplus$ : EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 24

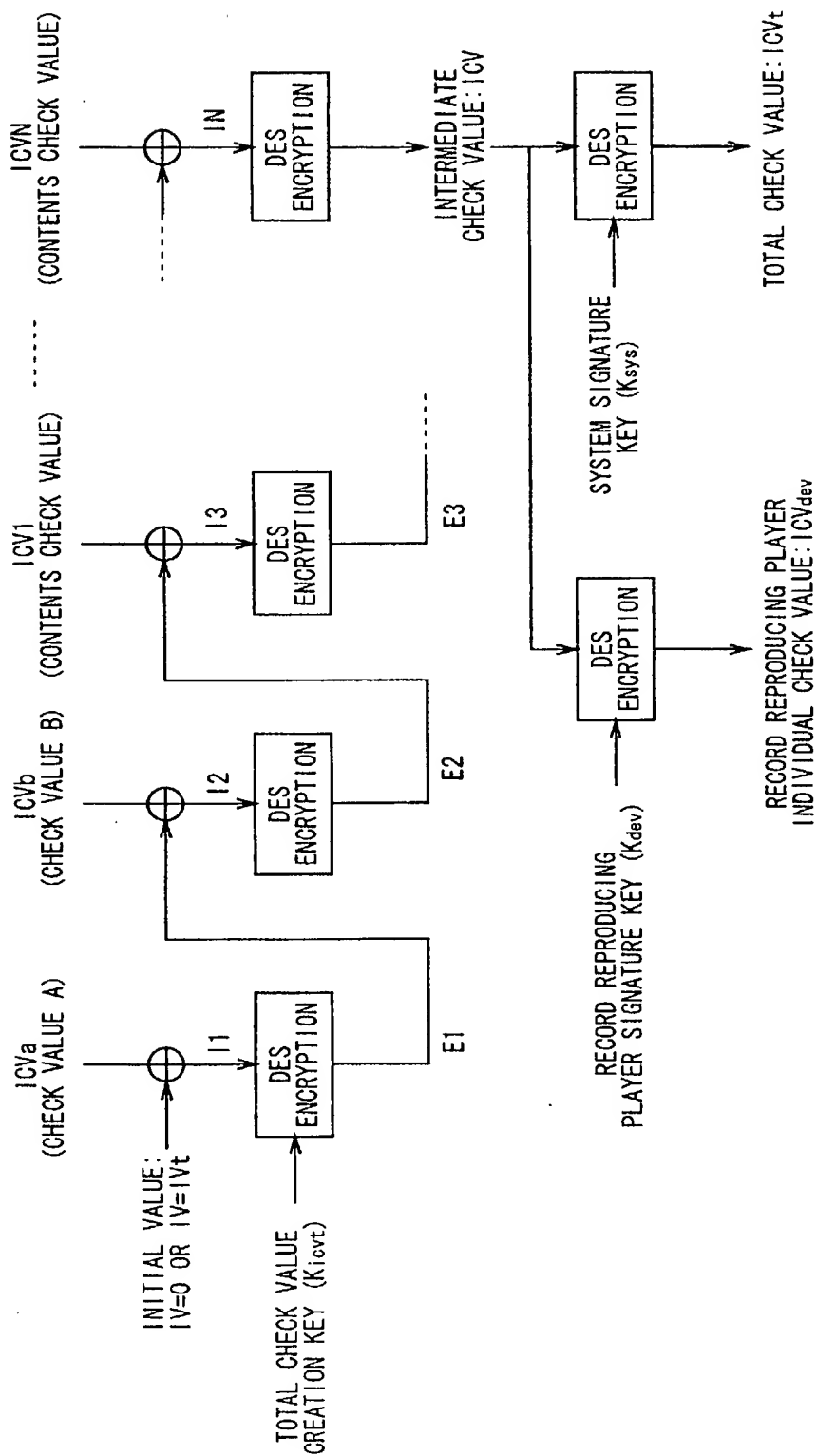
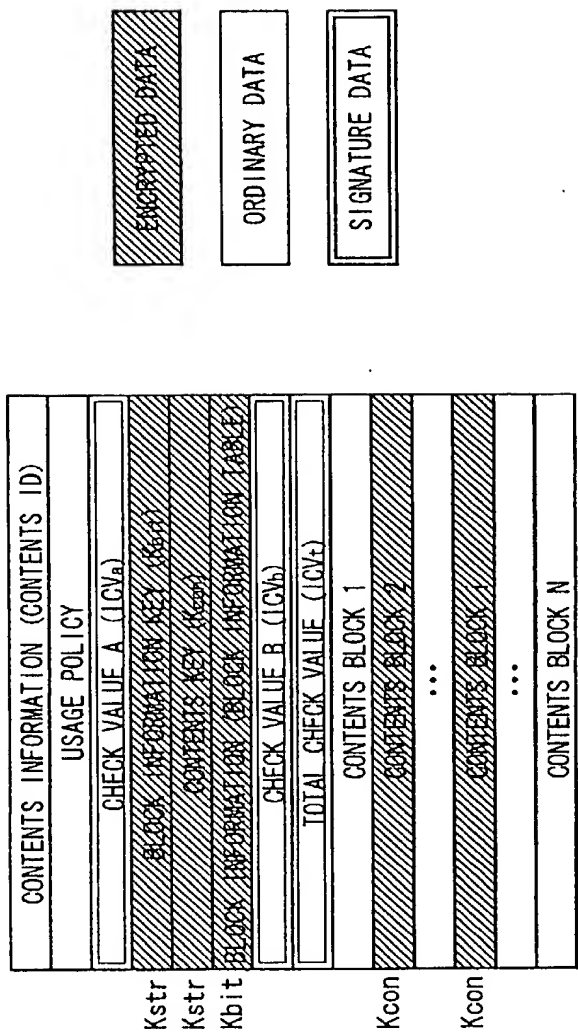
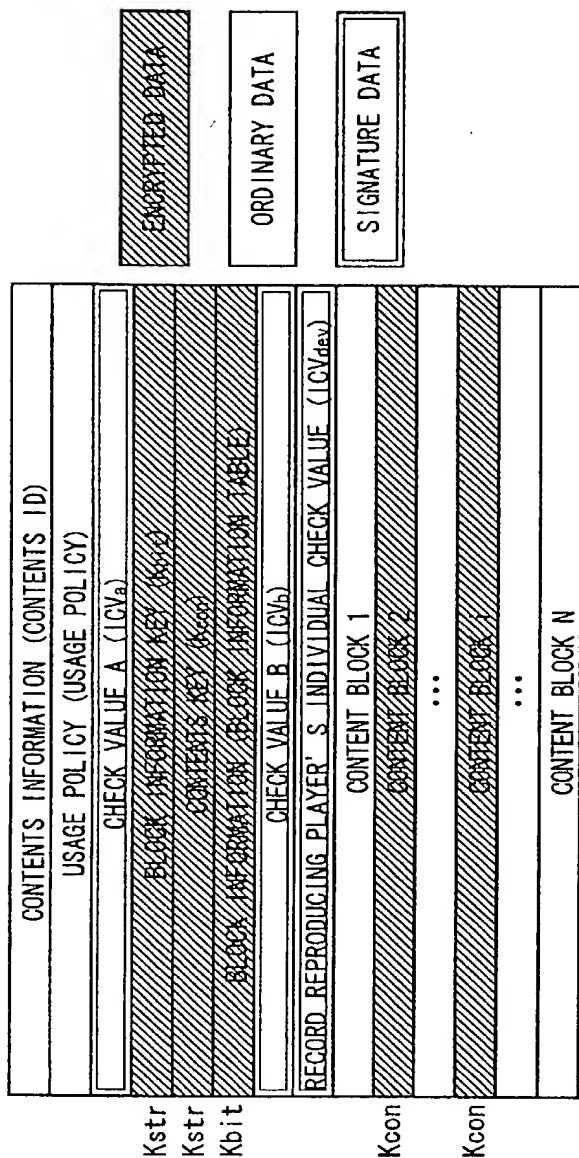


FIG. 25



CONTENTS SAVED IN RECORDING DEVICE  
(USE RESTRICTION INFORMATION = 0)

FIG. 26



CONTENTS SAVED IN RECORDING DEVICE  
(USE RESTRICTION INFORMATION = 1)

FIG. 27

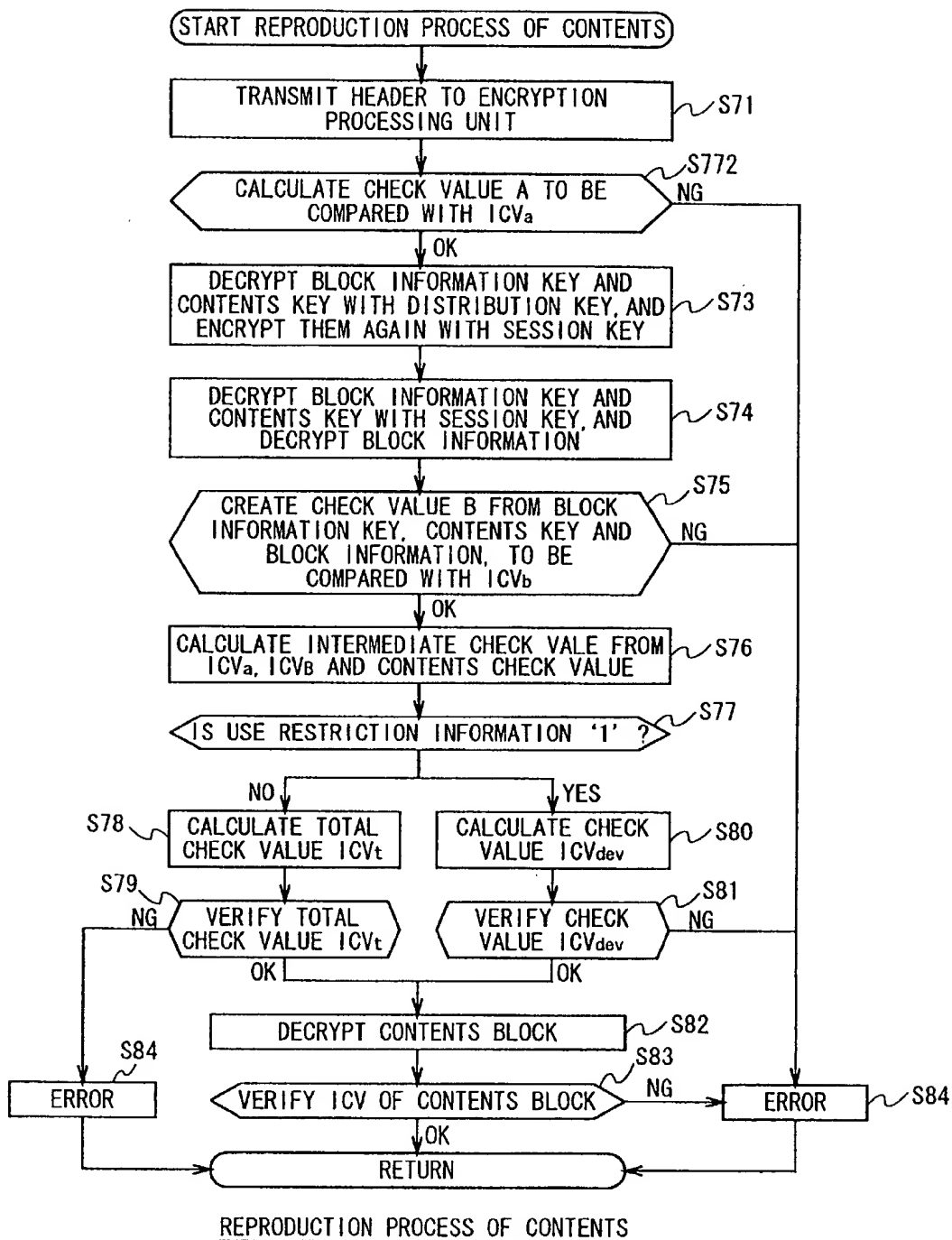


FIG. 28

FIG. 29

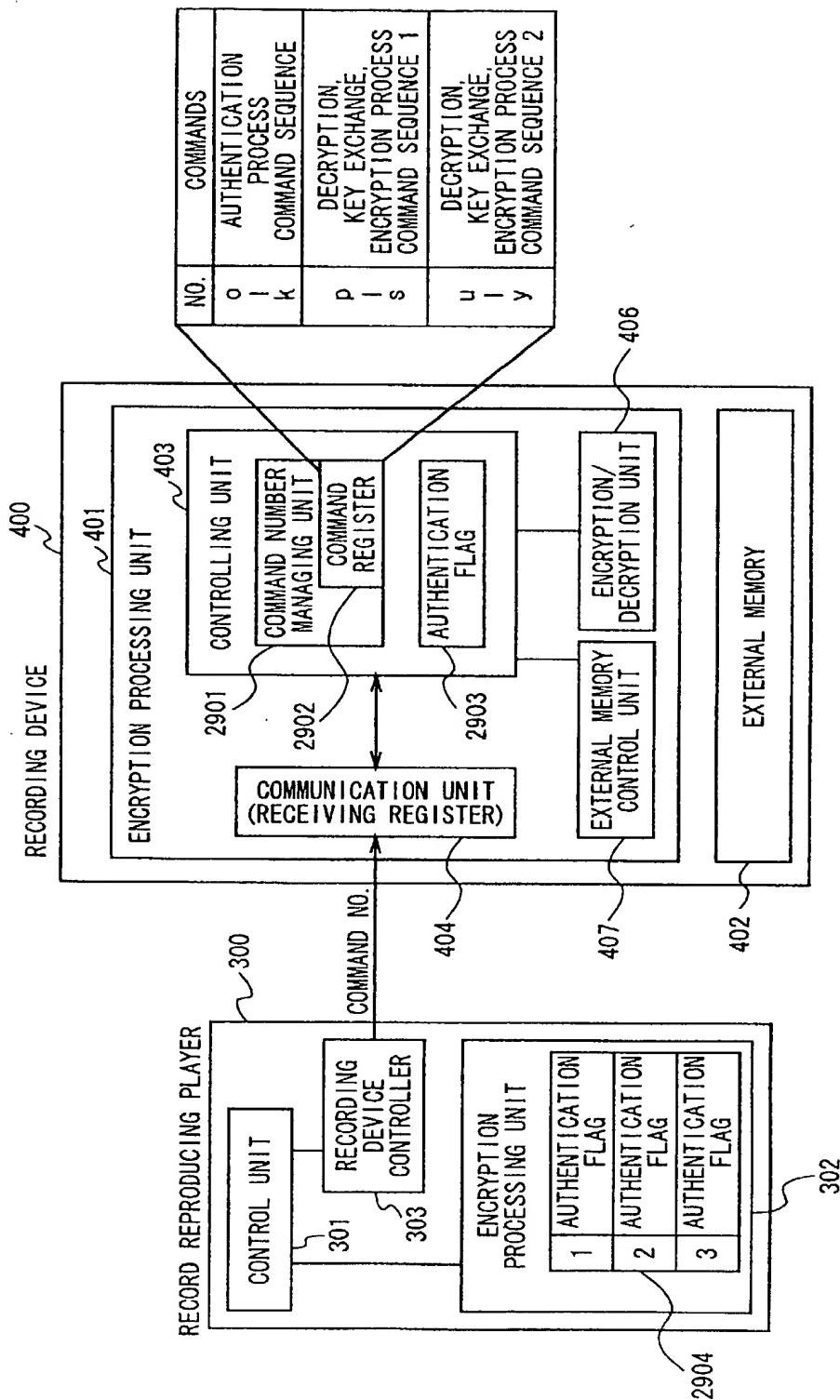


FIG. 29

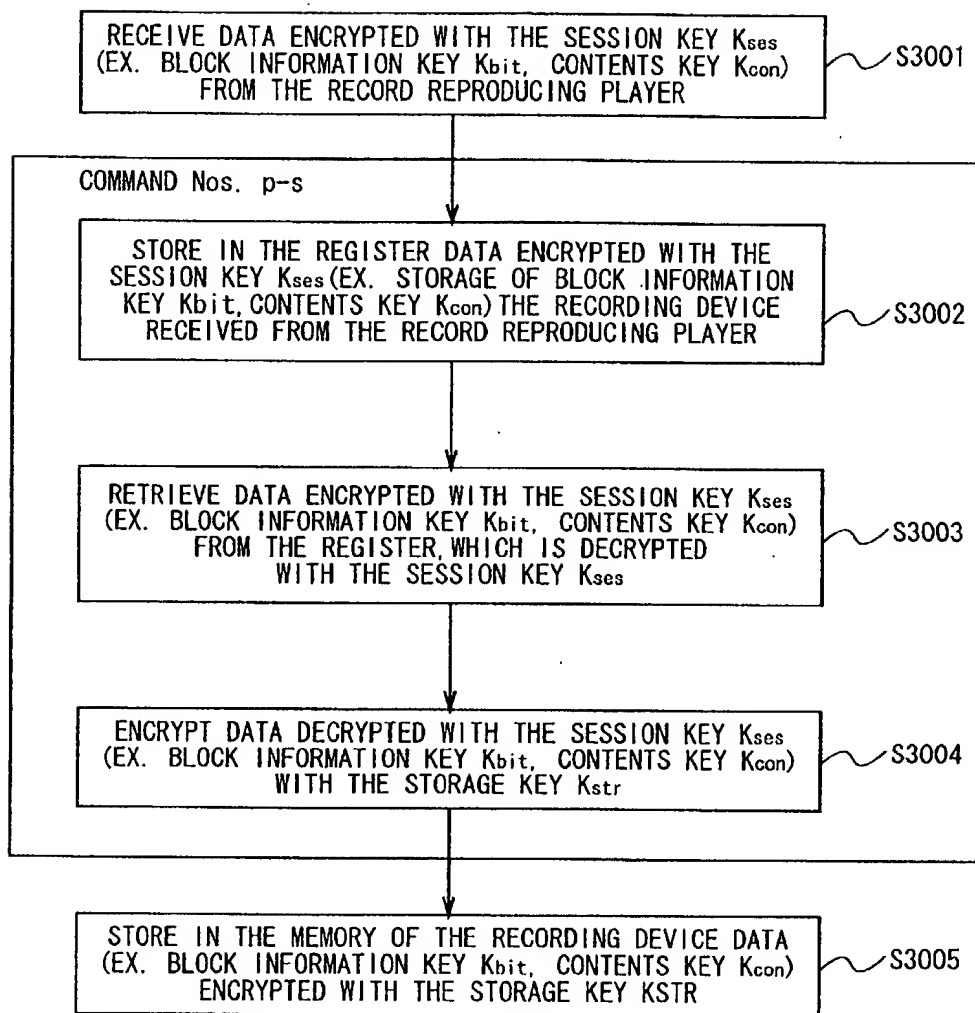


FIG. 30

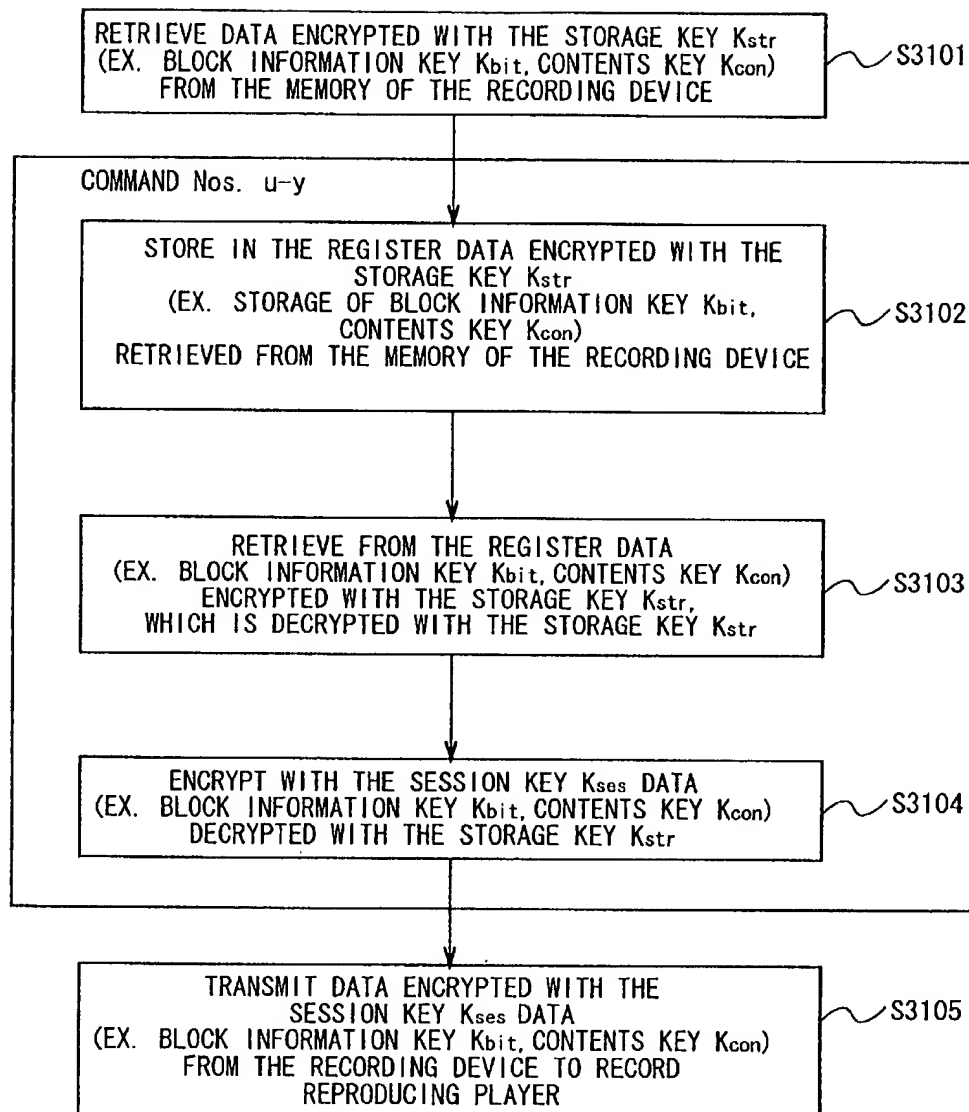
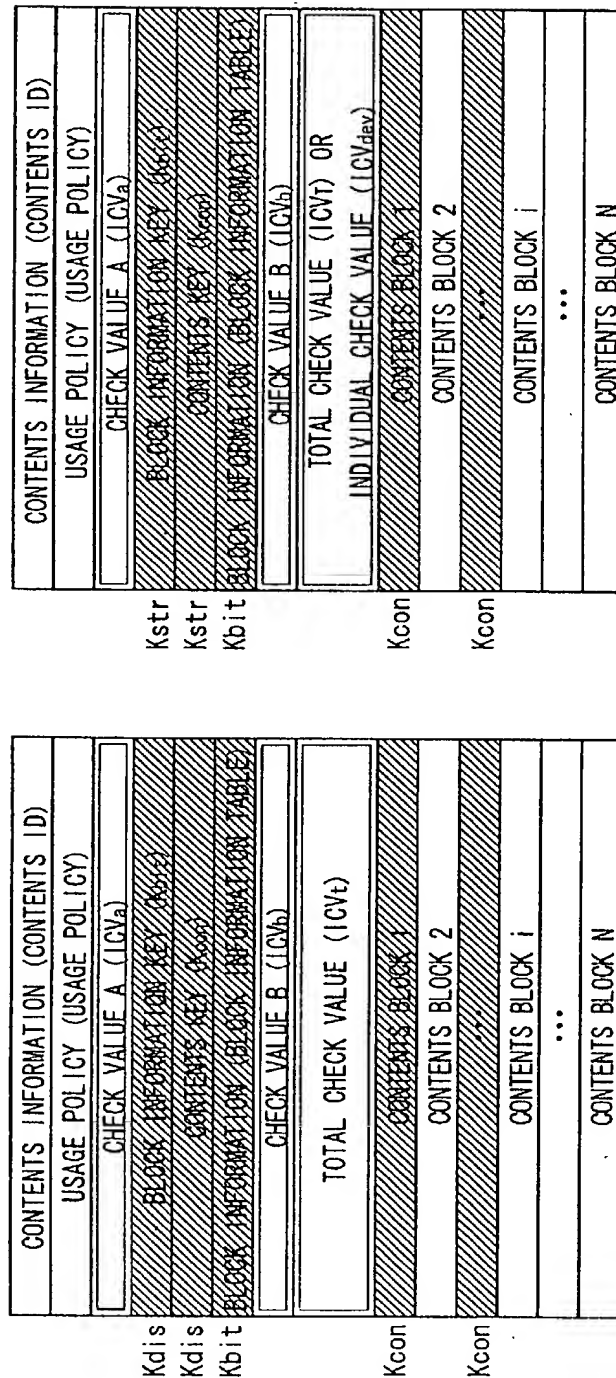


FIG. 31

FORMAT TYPE 0



DATA FORMAT ON MEDIA AND COMMUNICATION ROUTE      CONTENTS SAVED ON RECORDING DEVICE

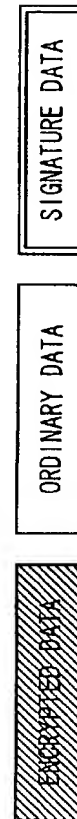


FIG. 32

09/937410

FORMAT TYPE 1

FORMAT TYPE 1

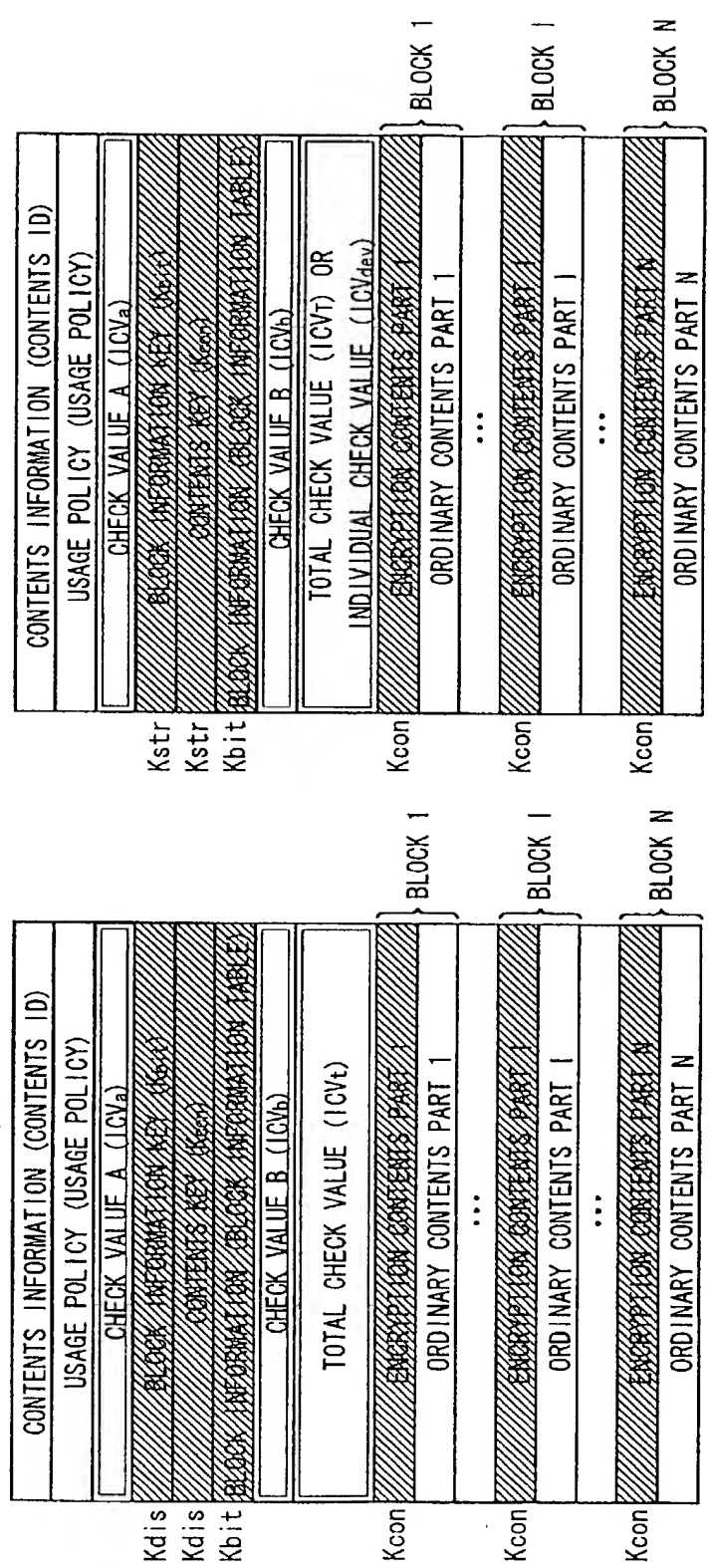
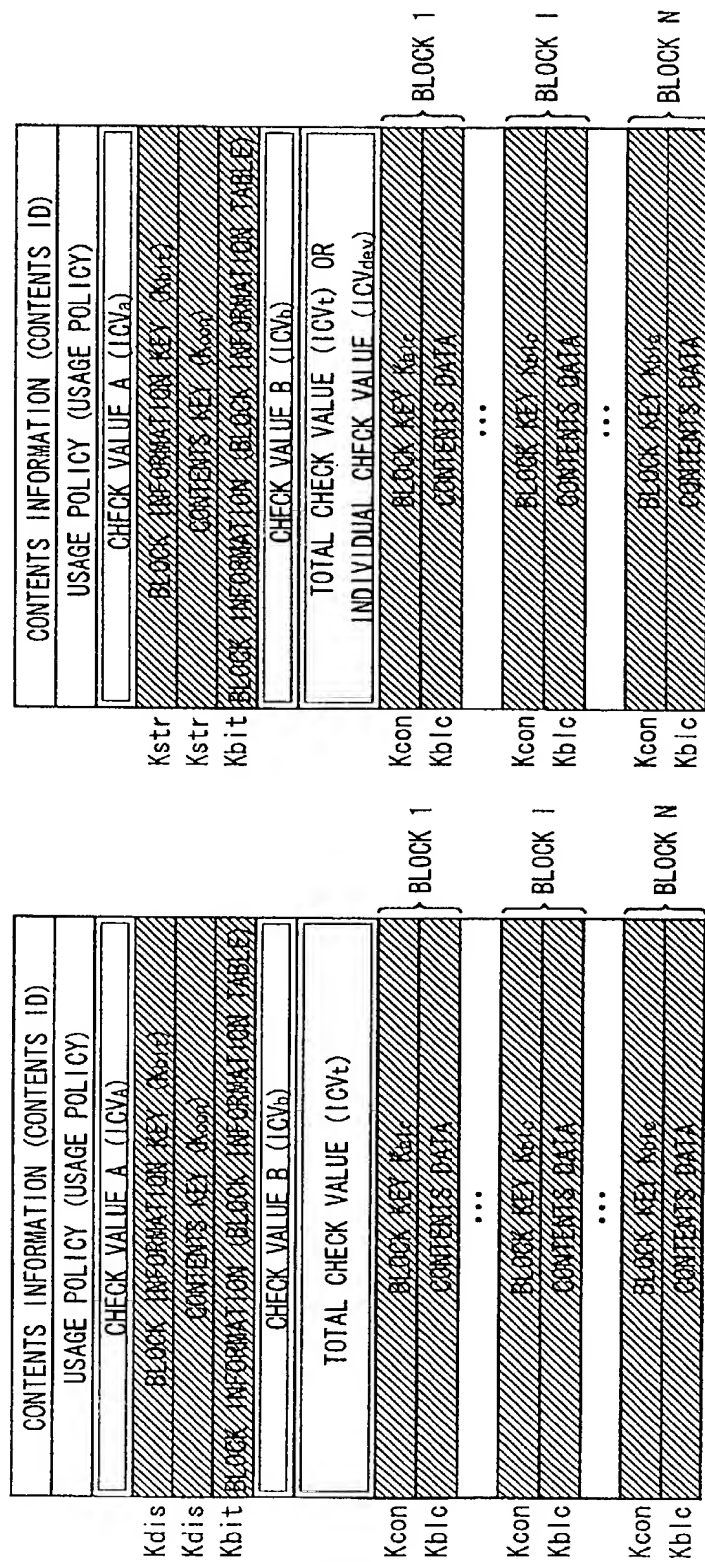


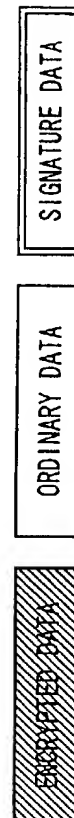
FIG. 33

## FORMAT TYPE 2



34/93

DATA FORMAT ON MEDIA AND COMMUNICATION ROUTE



**FIG. 34**

FORMAT TYPE 3

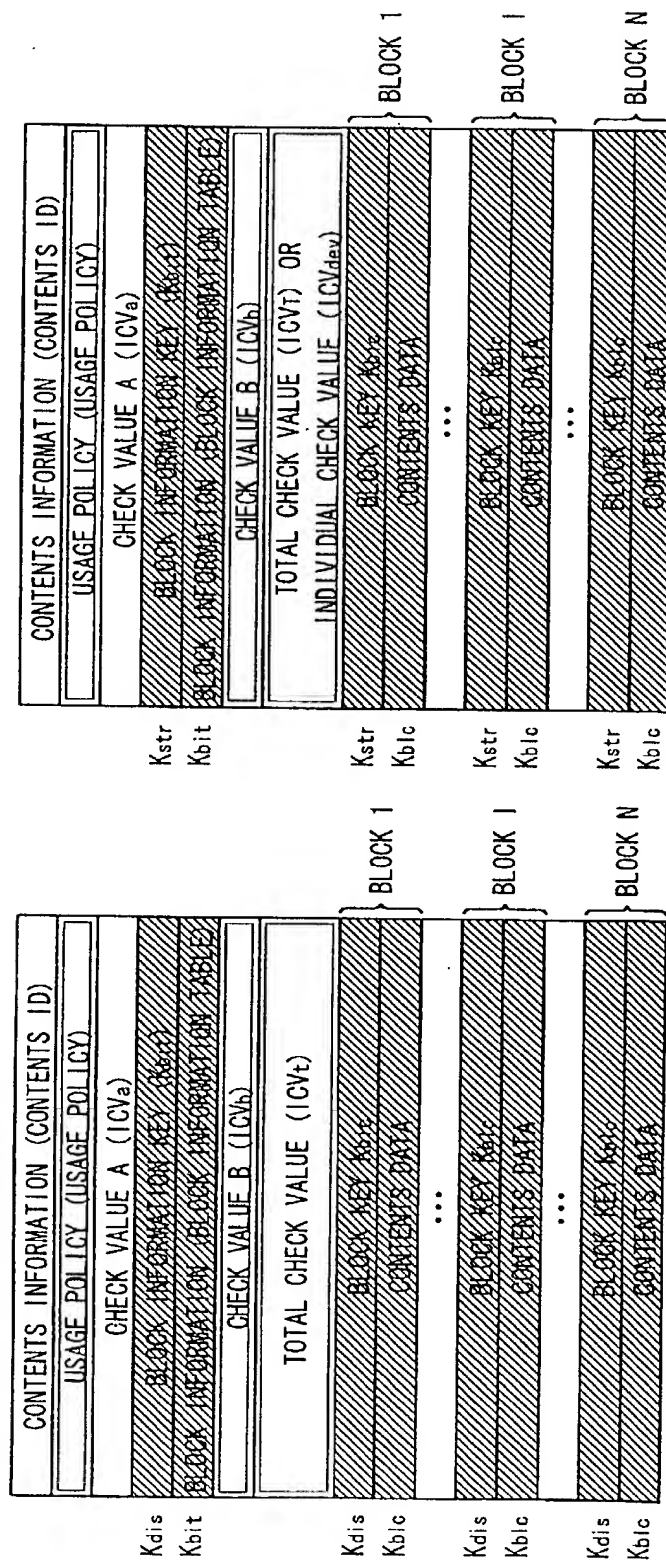
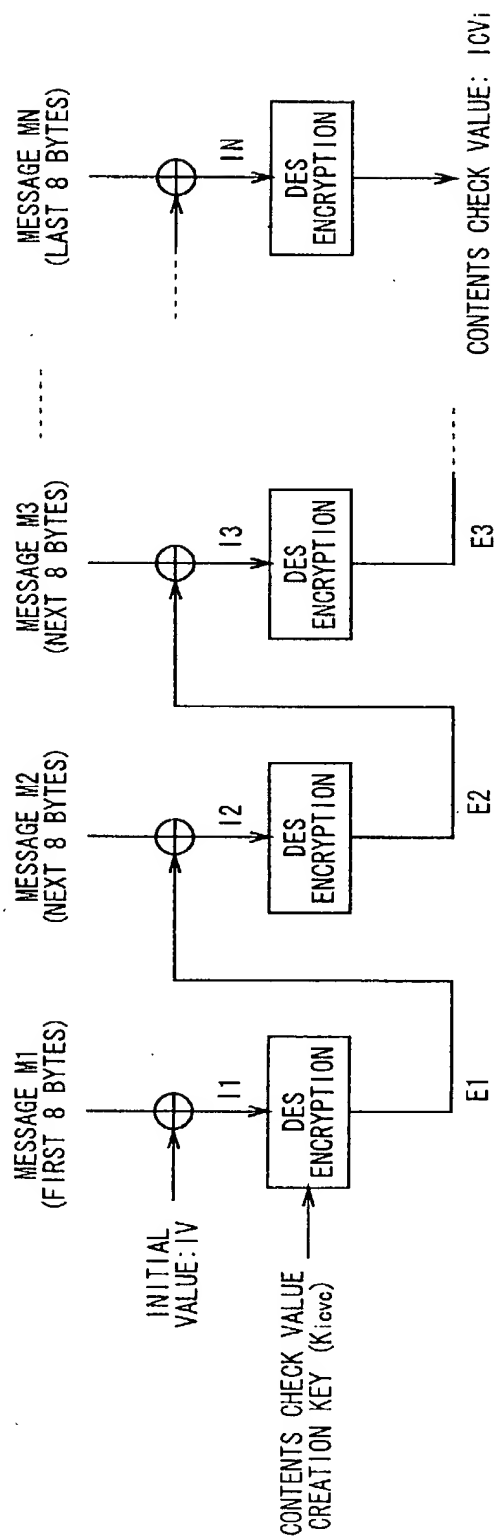


FIG. 35

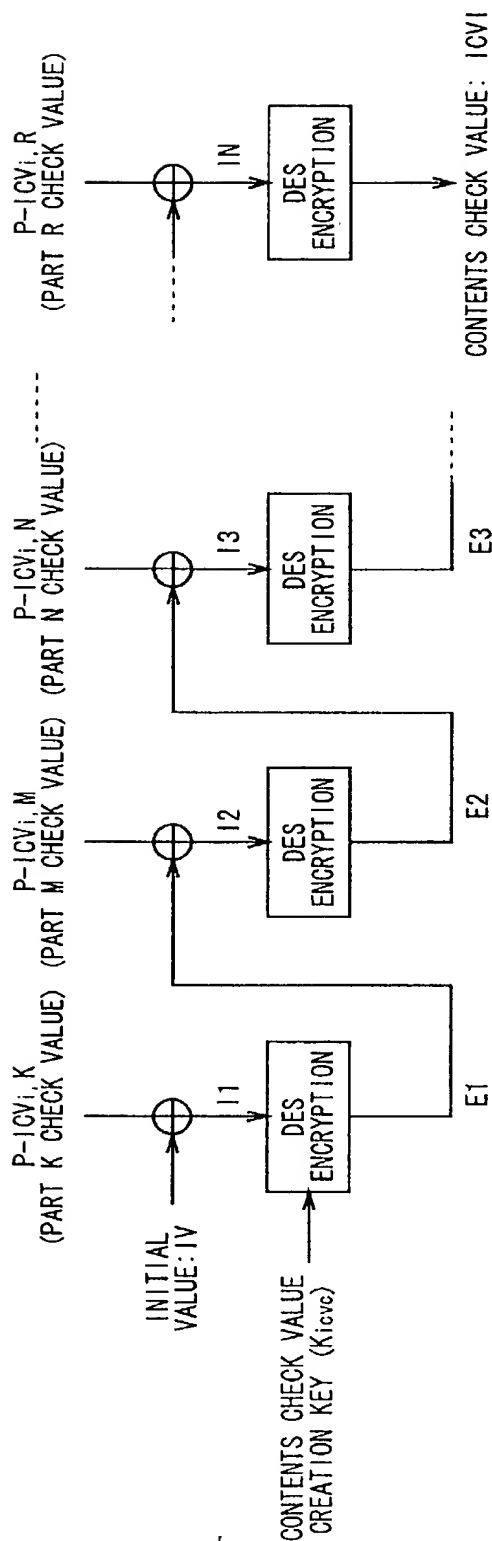


MESSAGE M1 - MN: CONTENTS DATE OF CONTENTS I

⊕: EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 36

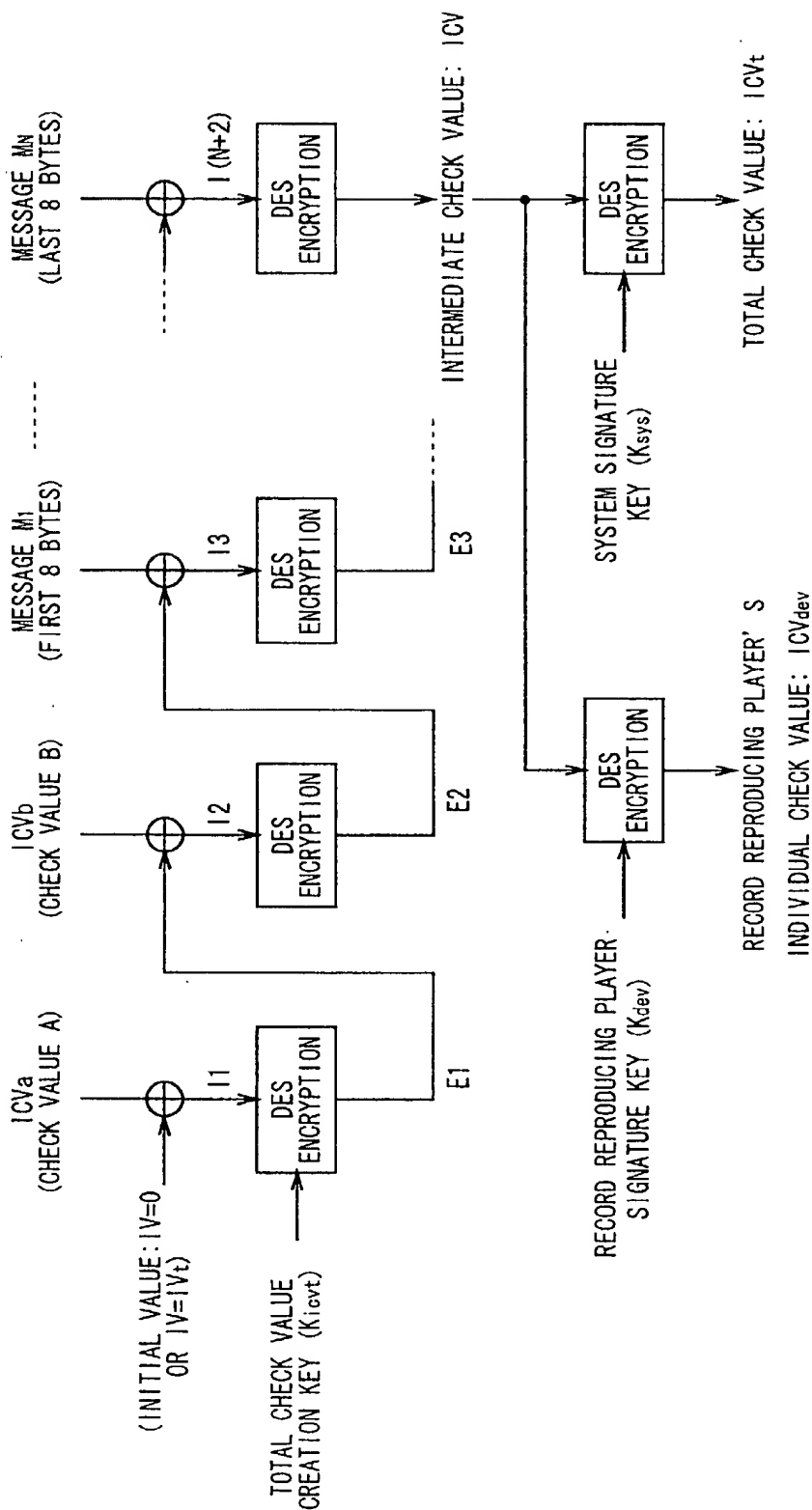
1002 0142E660



⊕: EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 37

09/937410



MESSAGE M<sub>1</sub> ~ M<sub>N</sub>: DATA OF CONTENTS BLOCK 1 ~ N

⊕: EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 38

## FORMAT TYPE 0, 1 DOWNLOADING PROCESS

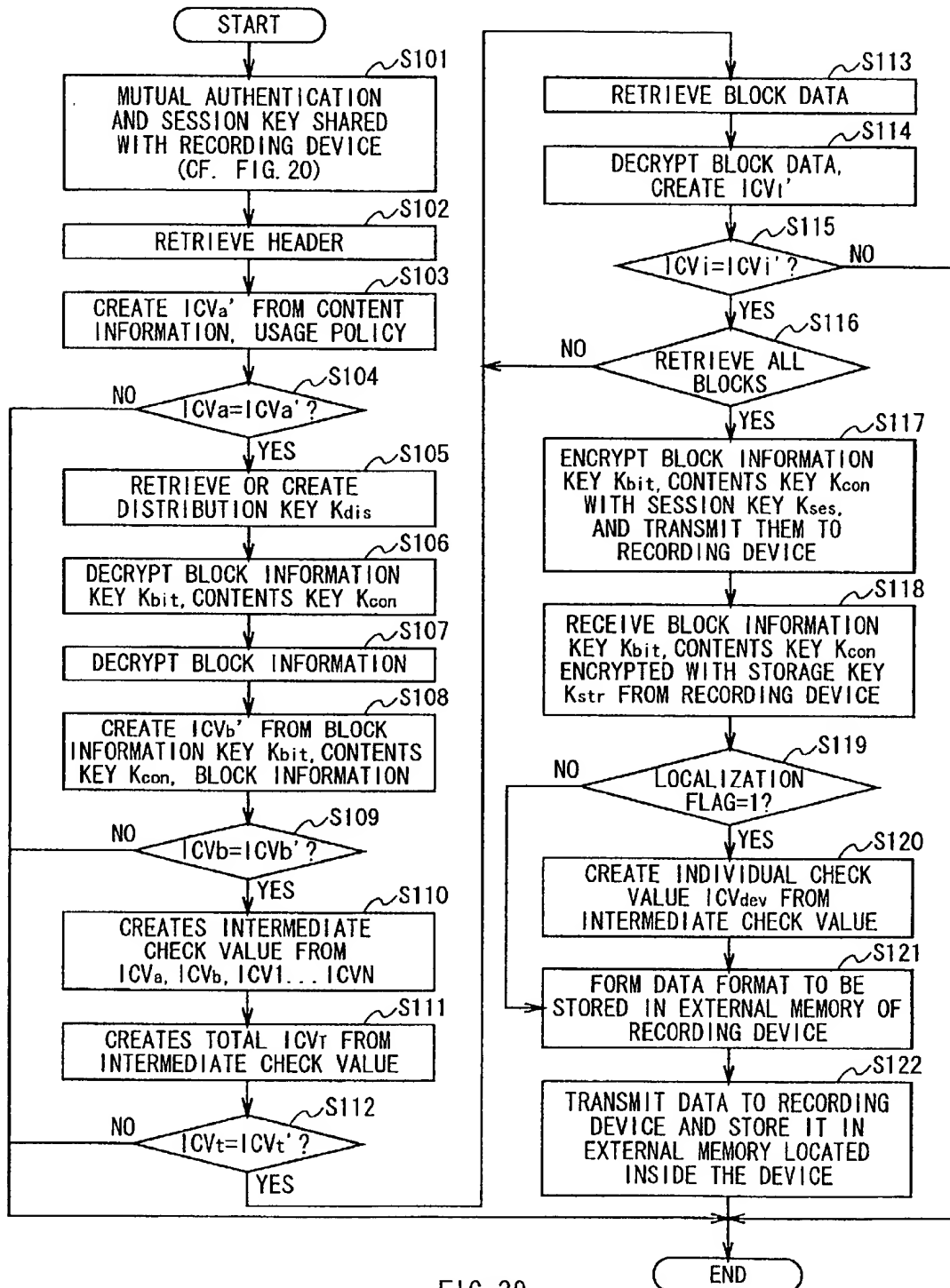


FIG. 39

## FORMAT TYPE 2 DOWNLOADING PROCESS

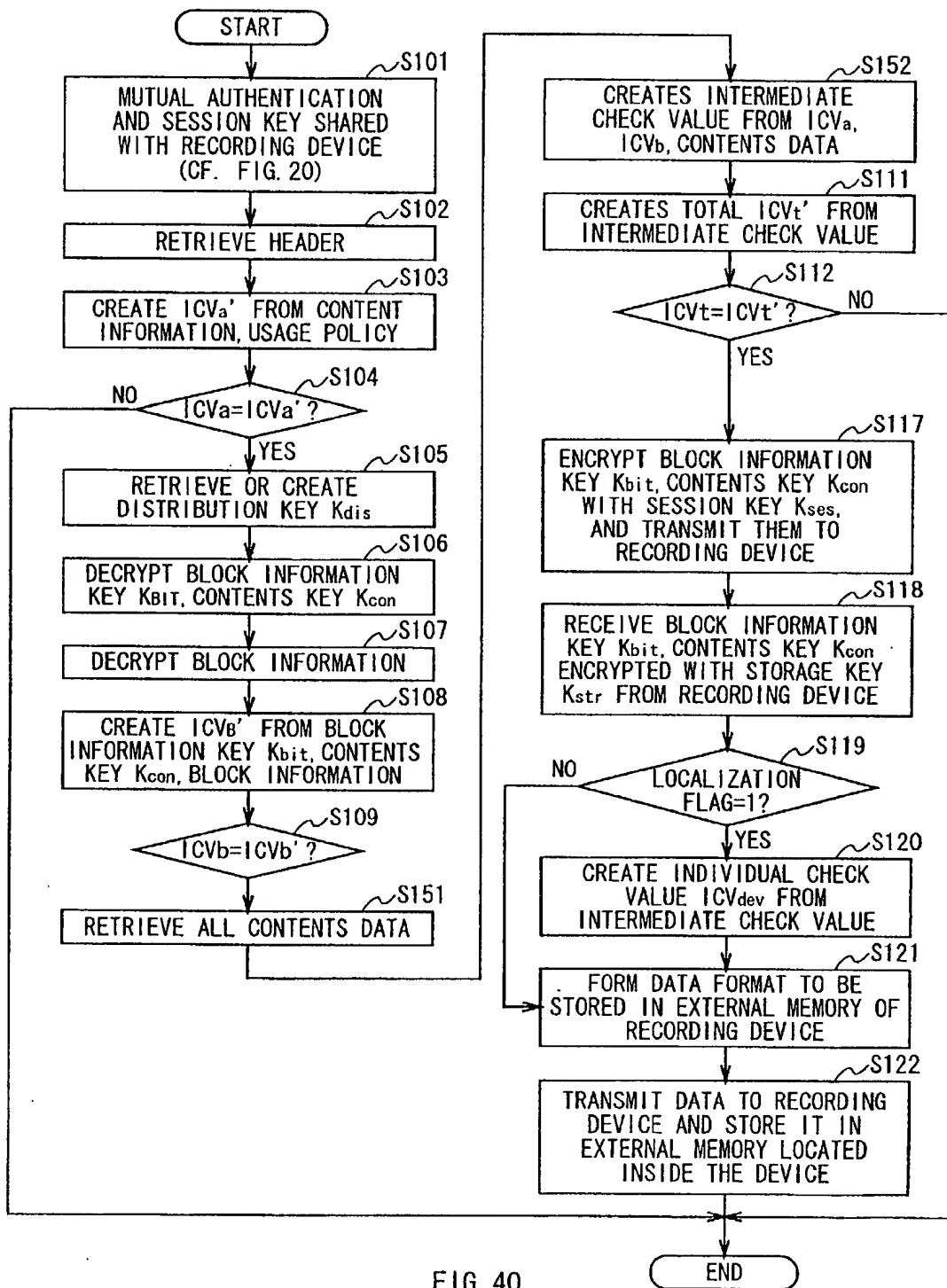


FIG. 40

## FORMAT TYPE 3 DOWNLOADING PROCESS

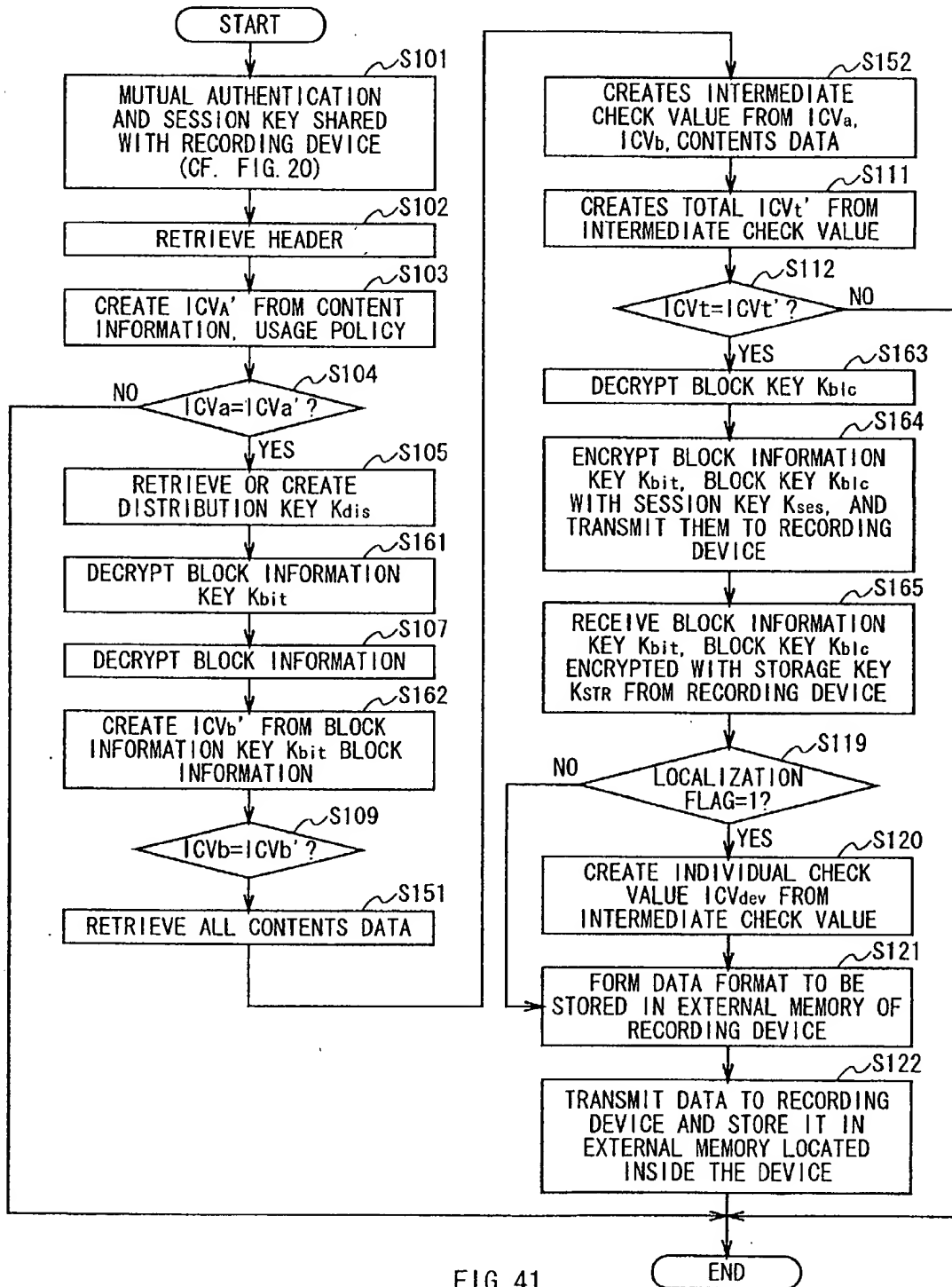
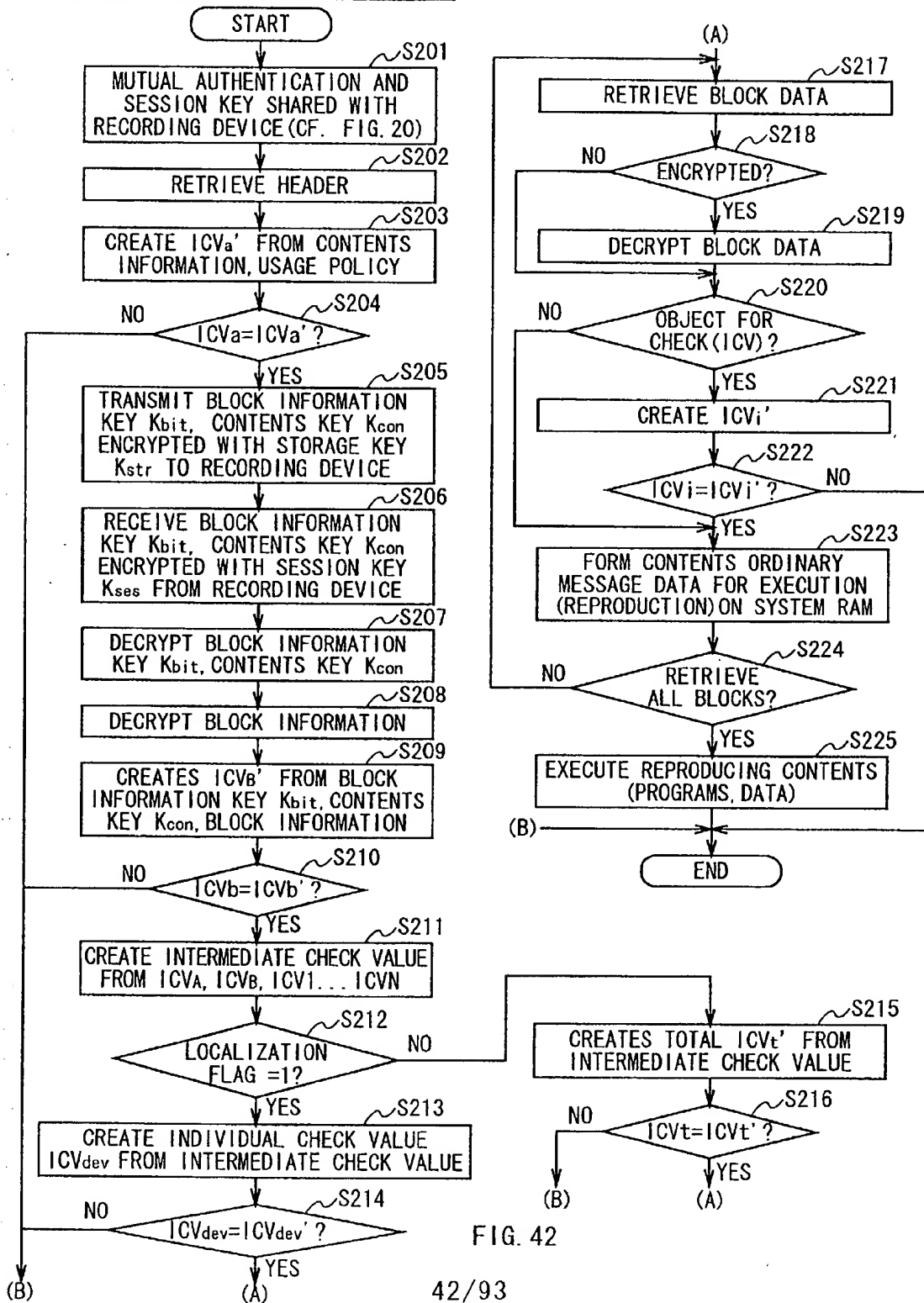
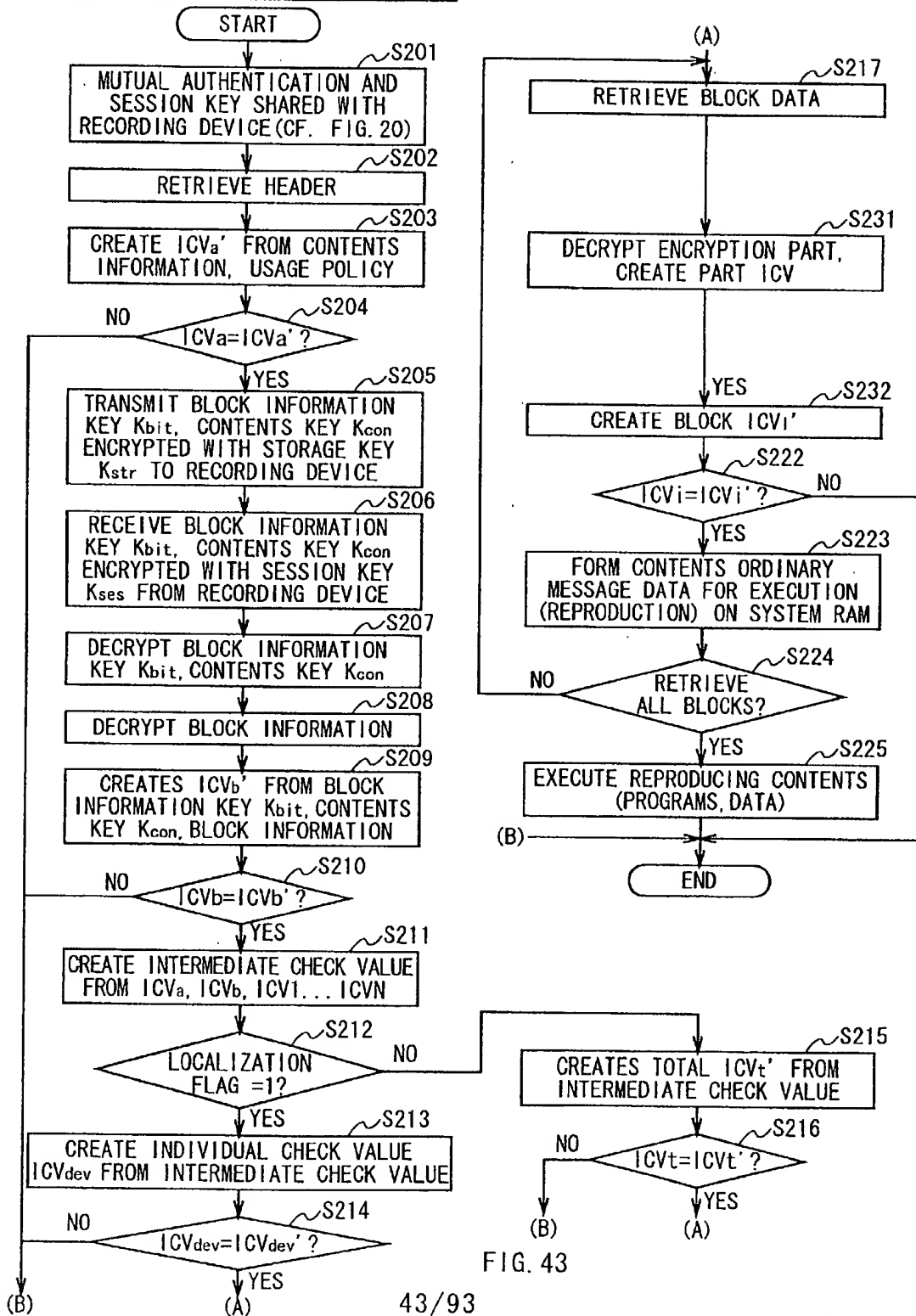


FIG. 41

## FORMAT TYPE 4 DOWNLOADING PROCESS



## FORMAT TYPE 1 REPRODUCTION PROCESS



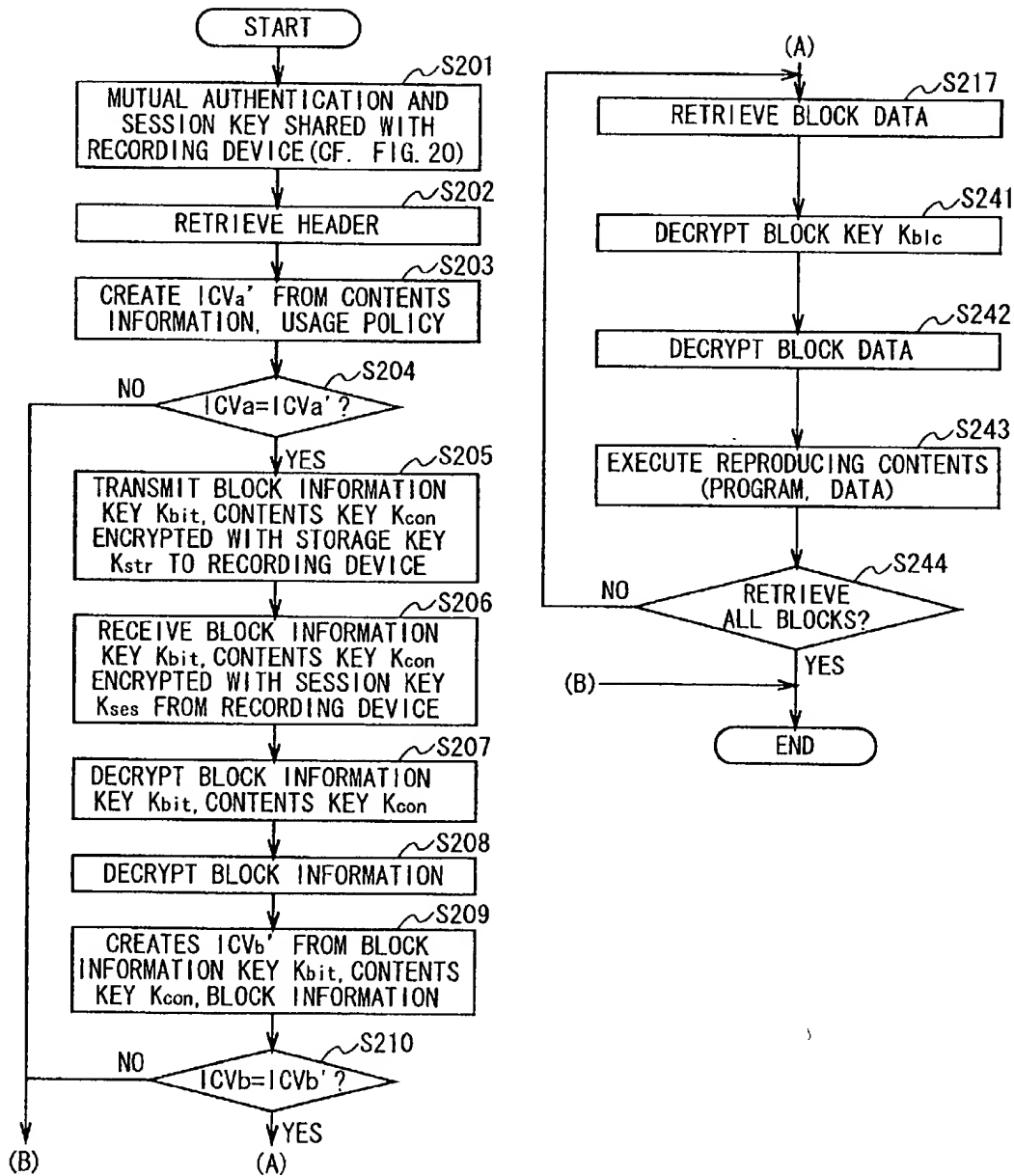


FIG. 44

## FORMAT TYPE 3 REPRODUCTION PROCESS

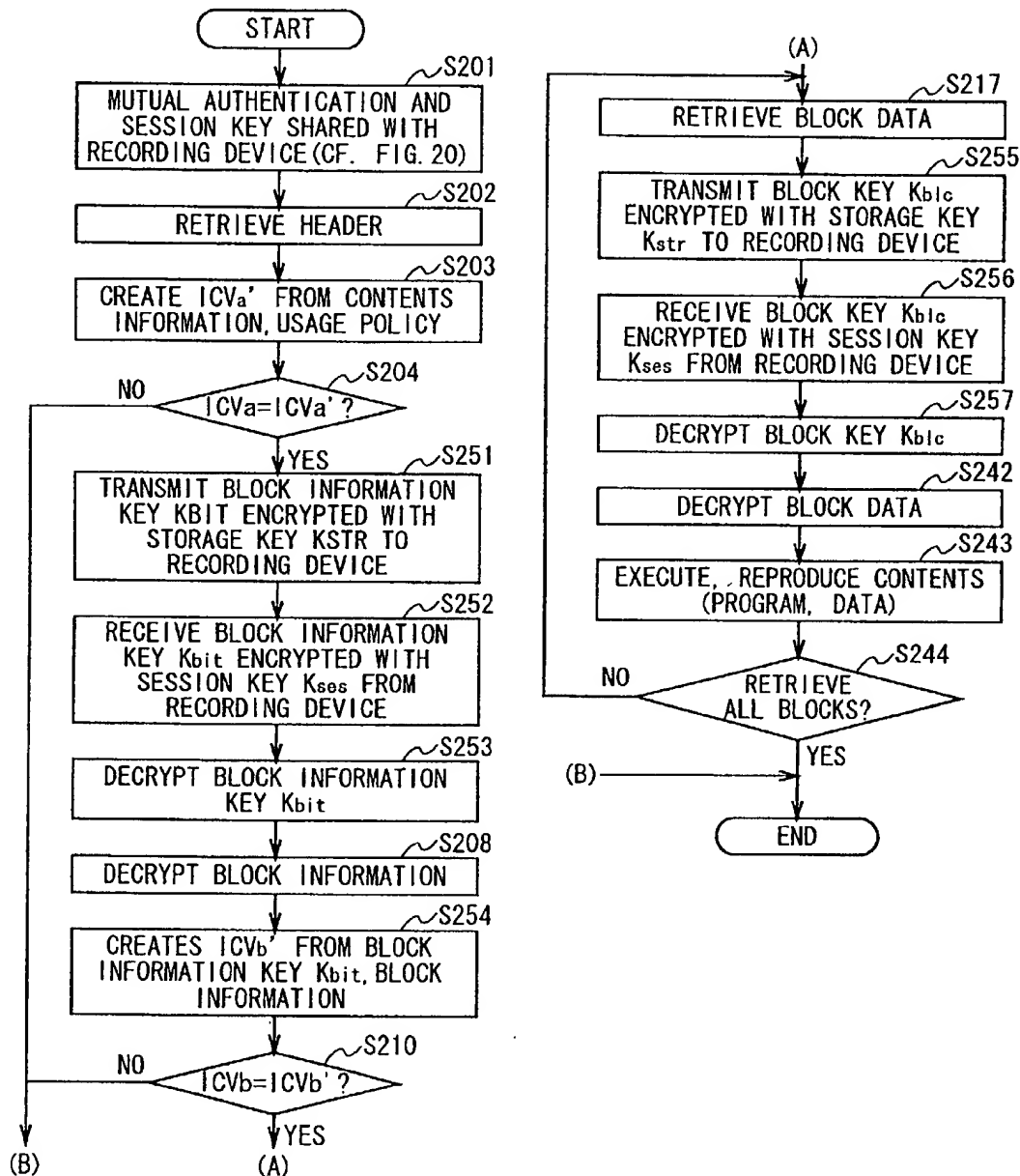


FIG. 45

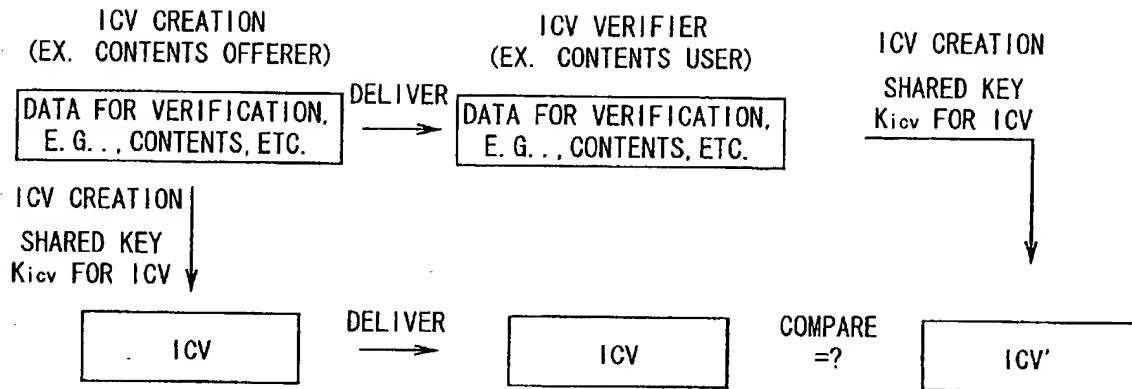


FIG. 46

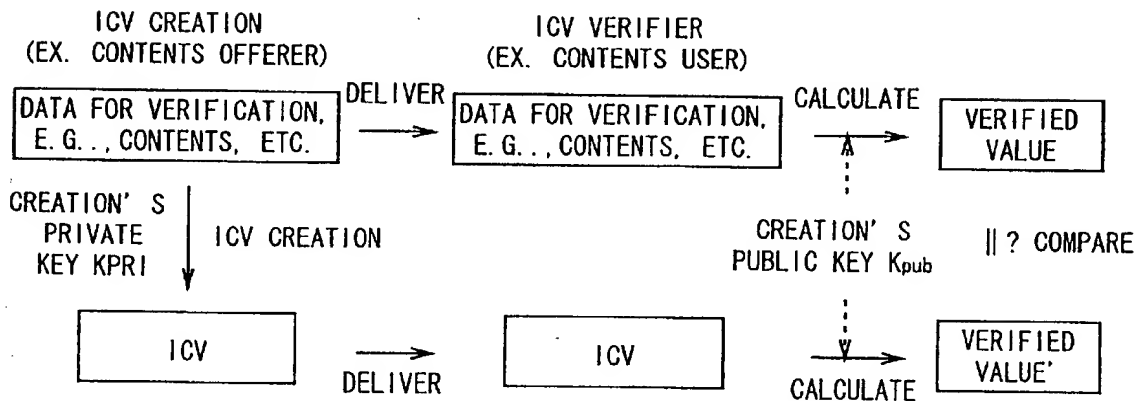


FIG. 47

FIG. 48

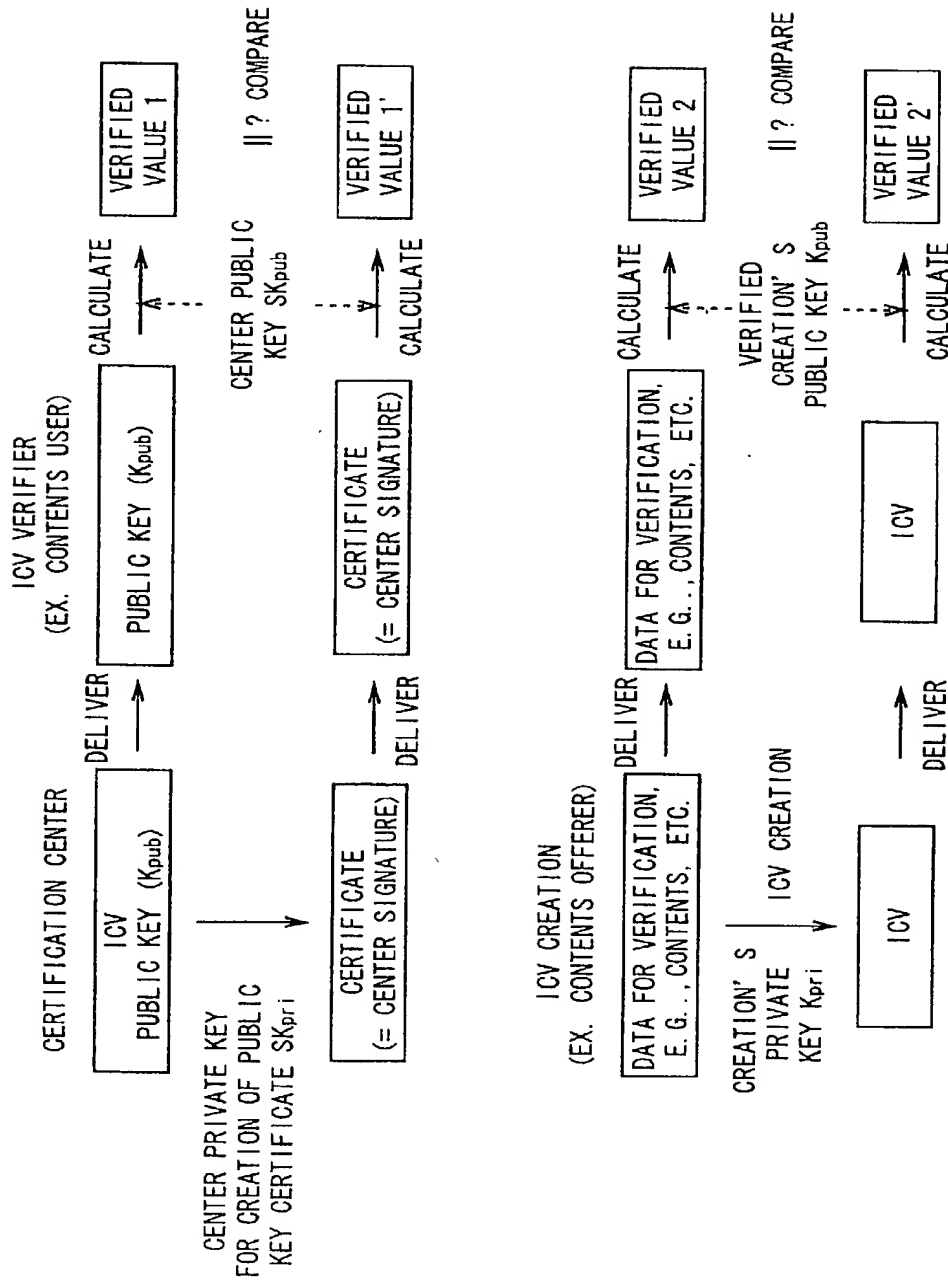


FIG. 48

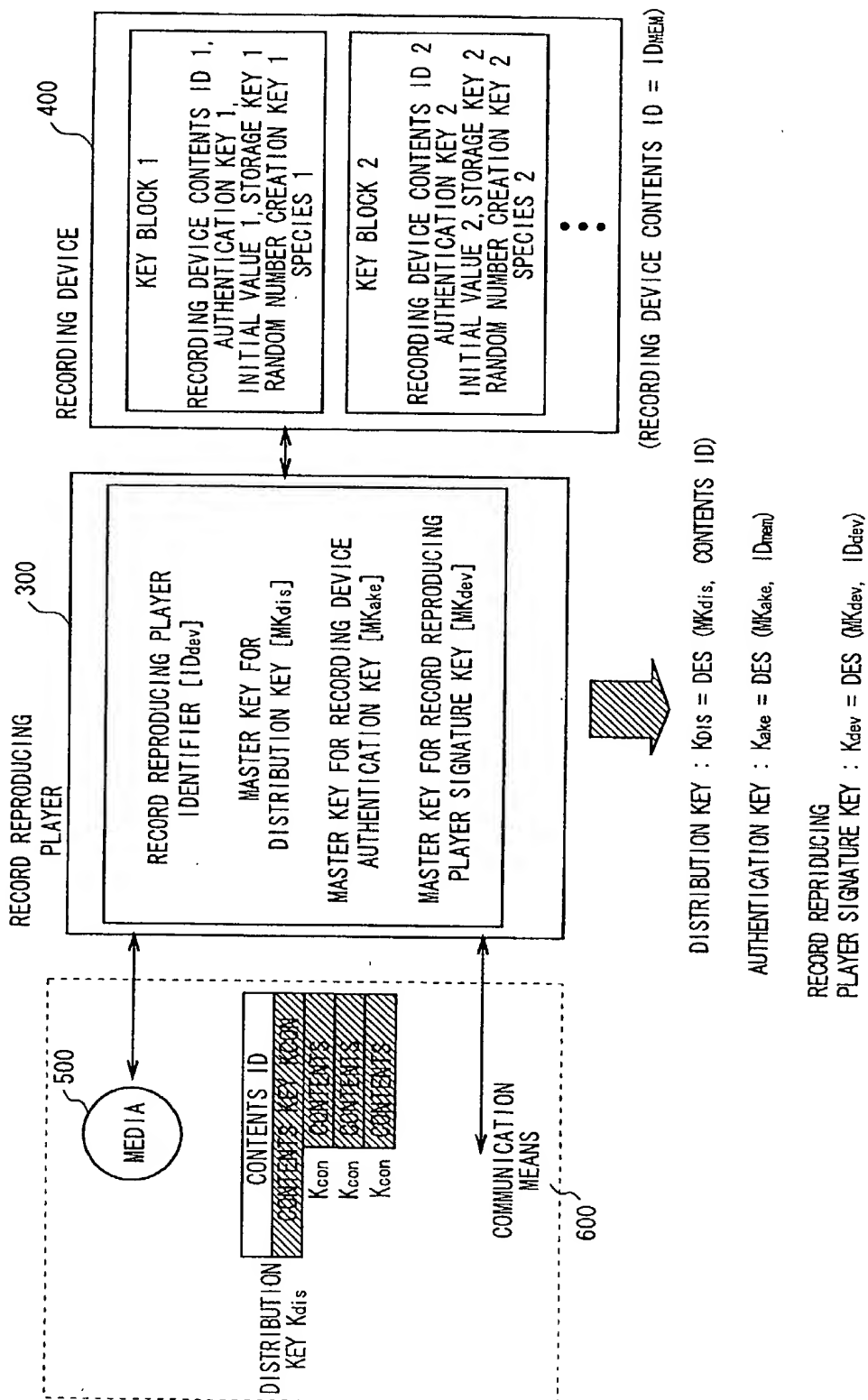
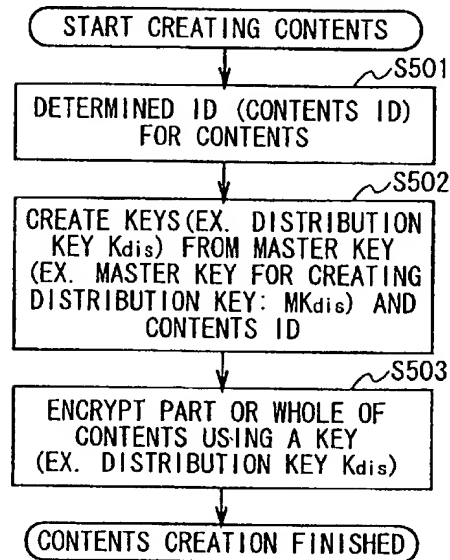


FIG. 49

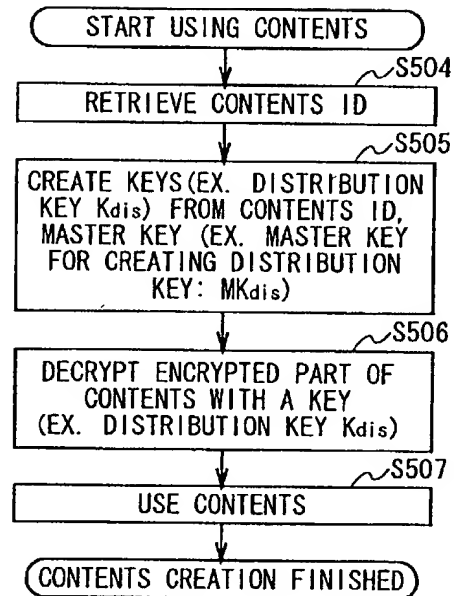
## METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY-(1)

## [BASIC FLOW]

## CONTENTS CREATION OR ADMINISTRATOR



## USER DEVICE



## [KEY POSSESSION COMPOSITION]

## CONTENTS CREATION OR ADMINISTRATOR

## USER DEVICE

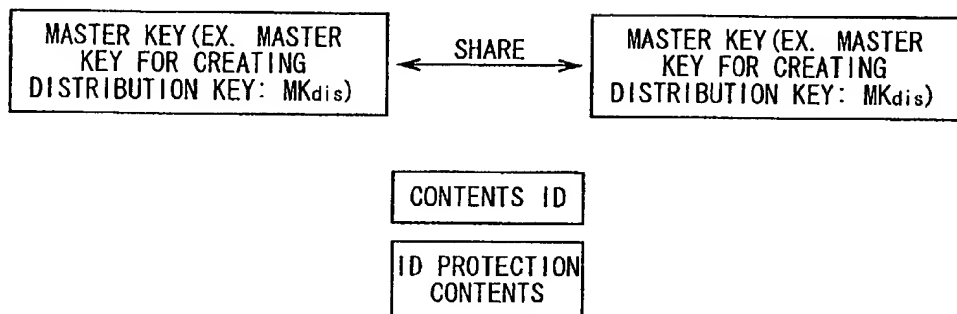


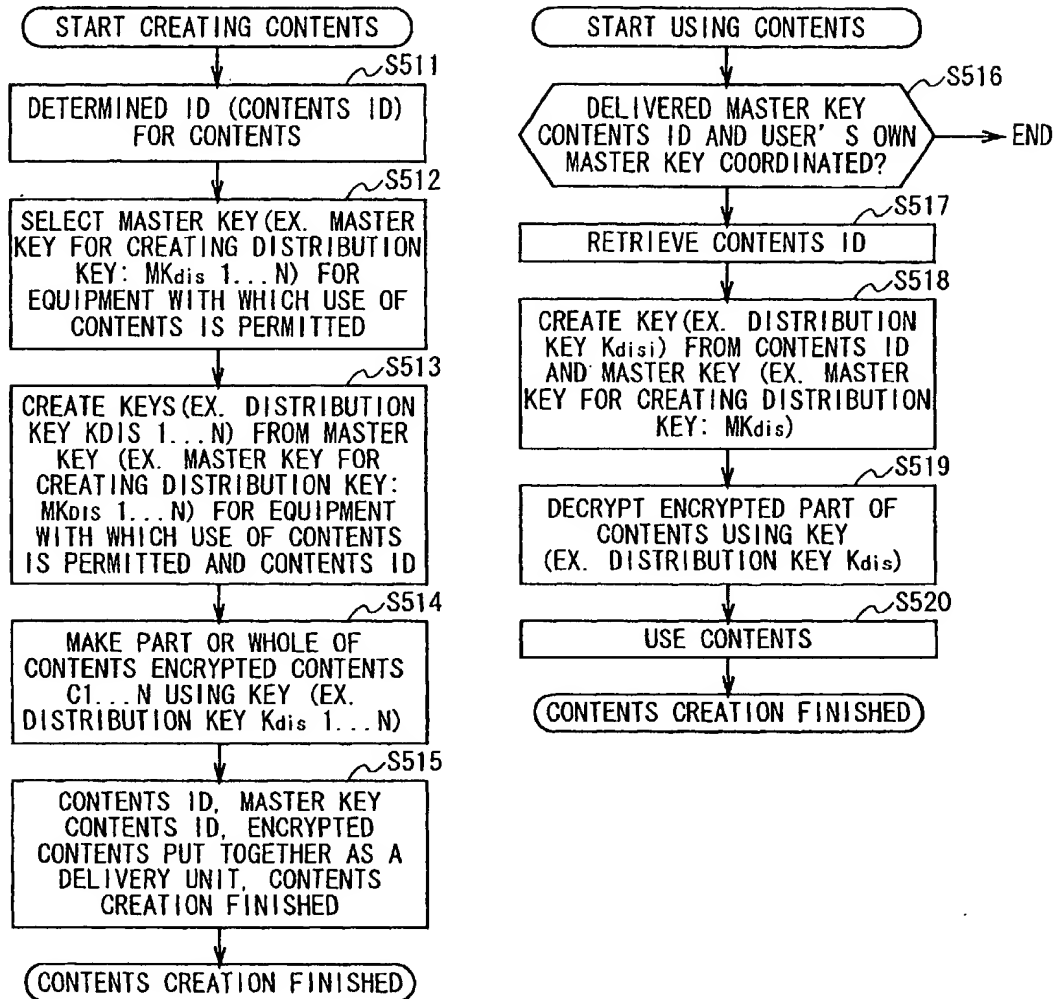
FIG. 50

## METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY-(2)

[BASIC FLOW]

CONTENTS CREATION OR ADMINISTRATOR

USER DEVICE



[KEY POSSESSION COMPOSITION]

CONTENTS CREATION OR ADMINISTRATOR

USER DEVICE

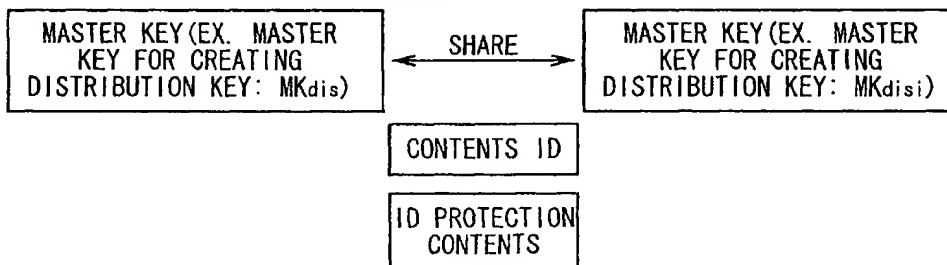


FIG. 51

FOUO: OFFICIAL

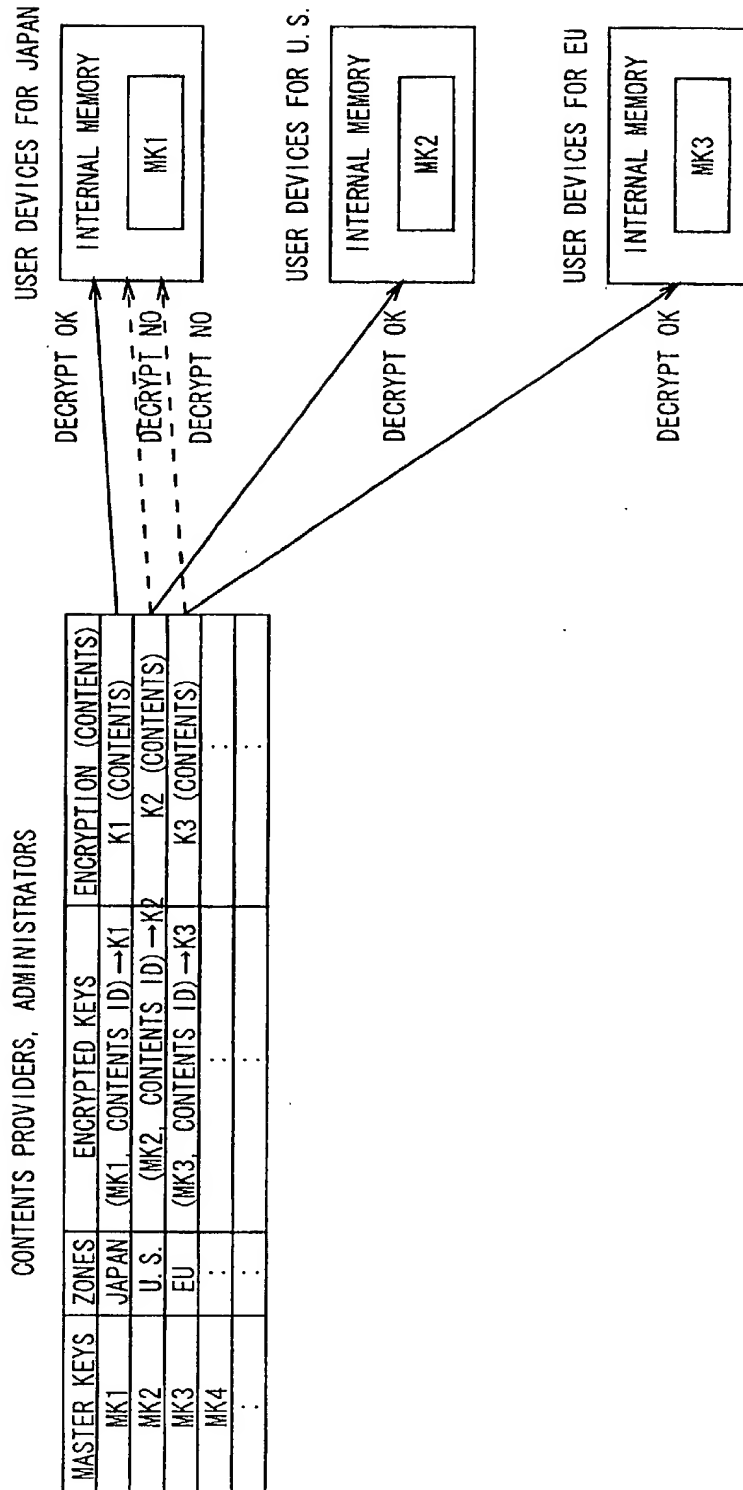
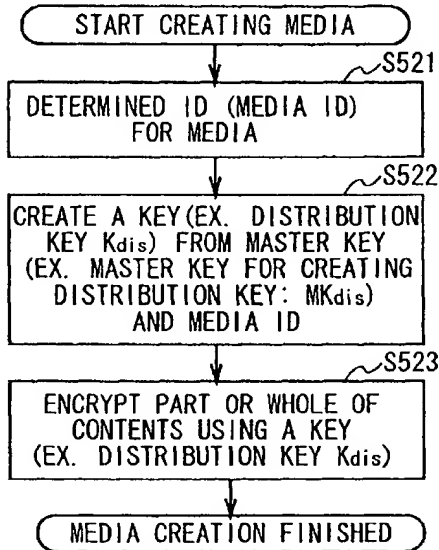


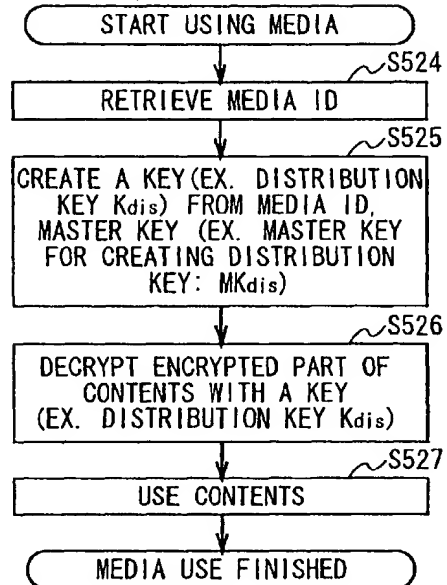
FIG. 52

METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY- (3)  
[BASIC FLOW]

MEDIA CREATION OR ADMINISTRATOR



USER DEVICE



[KEY POSSESSION COMPOSITION]

MEDIA CREATION OR ADMINISTRATOR

MASTER KEY (EX. MASTER KEY FOR CREATING DISTRIBUTION KEY: MKdis)

SHARE

USER DEVICE

MASTER KEY (EX. MASTER KEY FOR CREATING DISTRIBUTION KEY: MKdis)

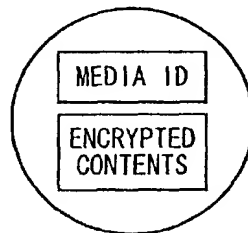
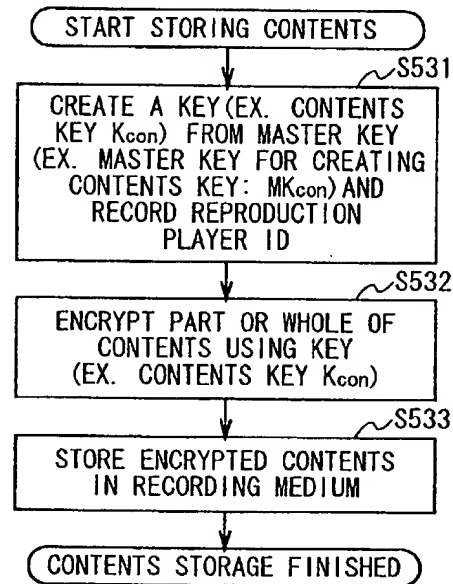


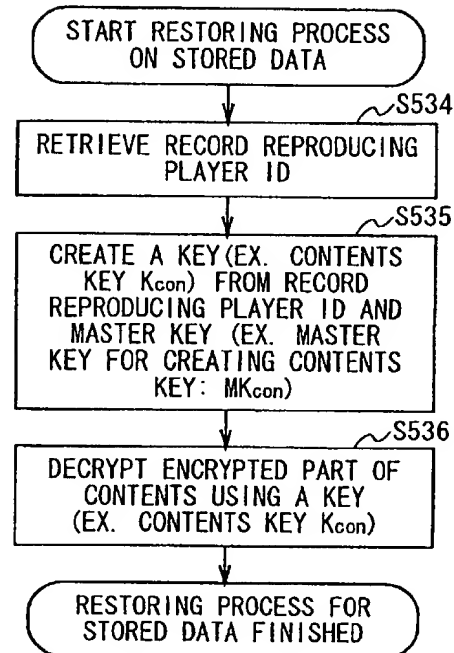
FIG. 53

METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY-(4)  
[BASIC FLOW]

RECORD REPRODUCING PLAYER USER



SYSTEM ADMINISTRATOR



[KEY POSSESSION COMPOSITION]

RECORD REPRODUCING PLAYER USER

MASTER KEY (EX. MASTER KEY FOR CREATING CONTENTS KEY: MKcon)

SHARE

SYSTEM ADMINISTRATOR

MASTER KEY (EX. MASTER KEY FOR CREATING CONTENTS KEY: Mcon)

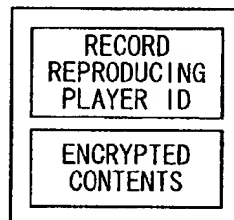
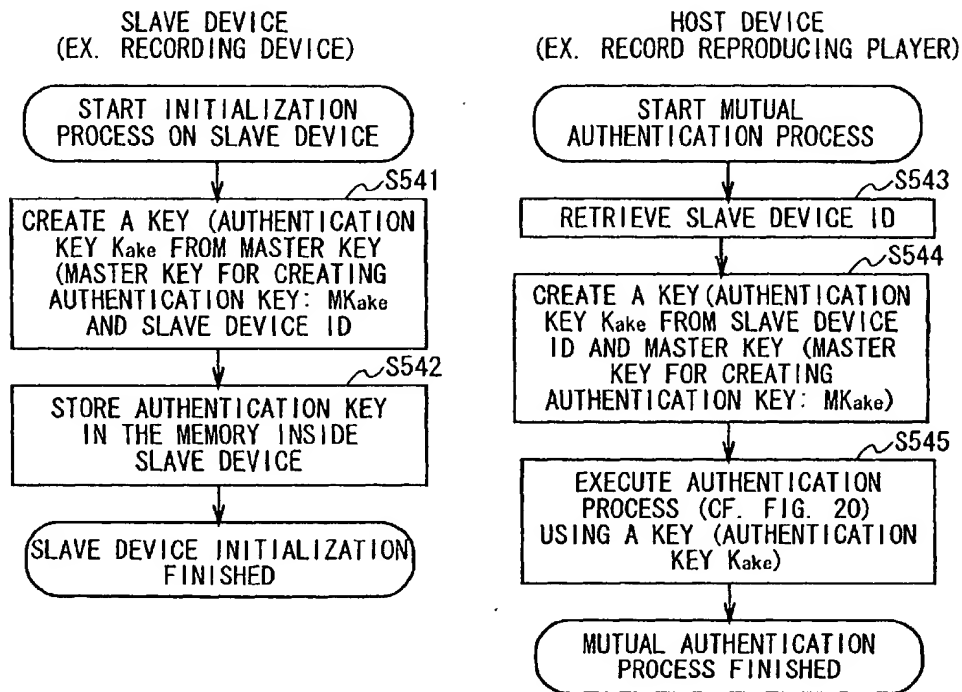


FIG. 54

METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY-(5)  
[BASIC FLOW]



[KEY POSSESSION COMPOSITION]

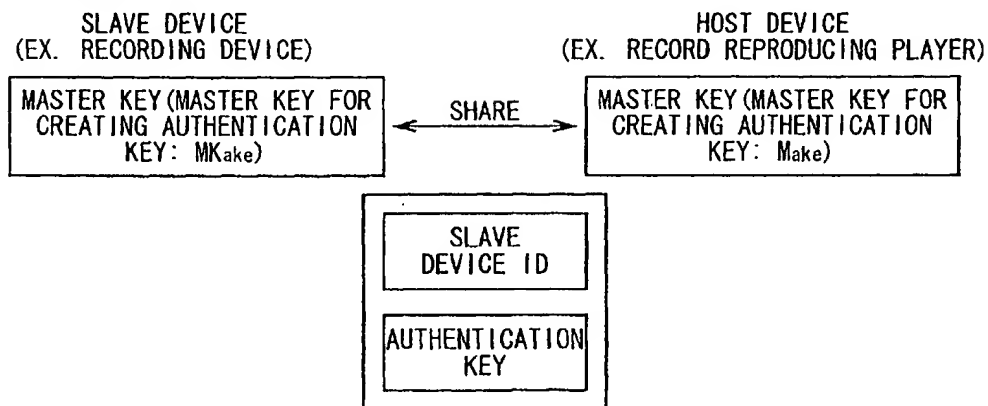


FIG. 55

STORING (DOWNLOADING) PROCESS OF  
TRIPLE DES-APPLIED CONTENTS KEYS:  $K_{c1}$ ,  $K_{c2}$ , ( $K_{c3}$ )

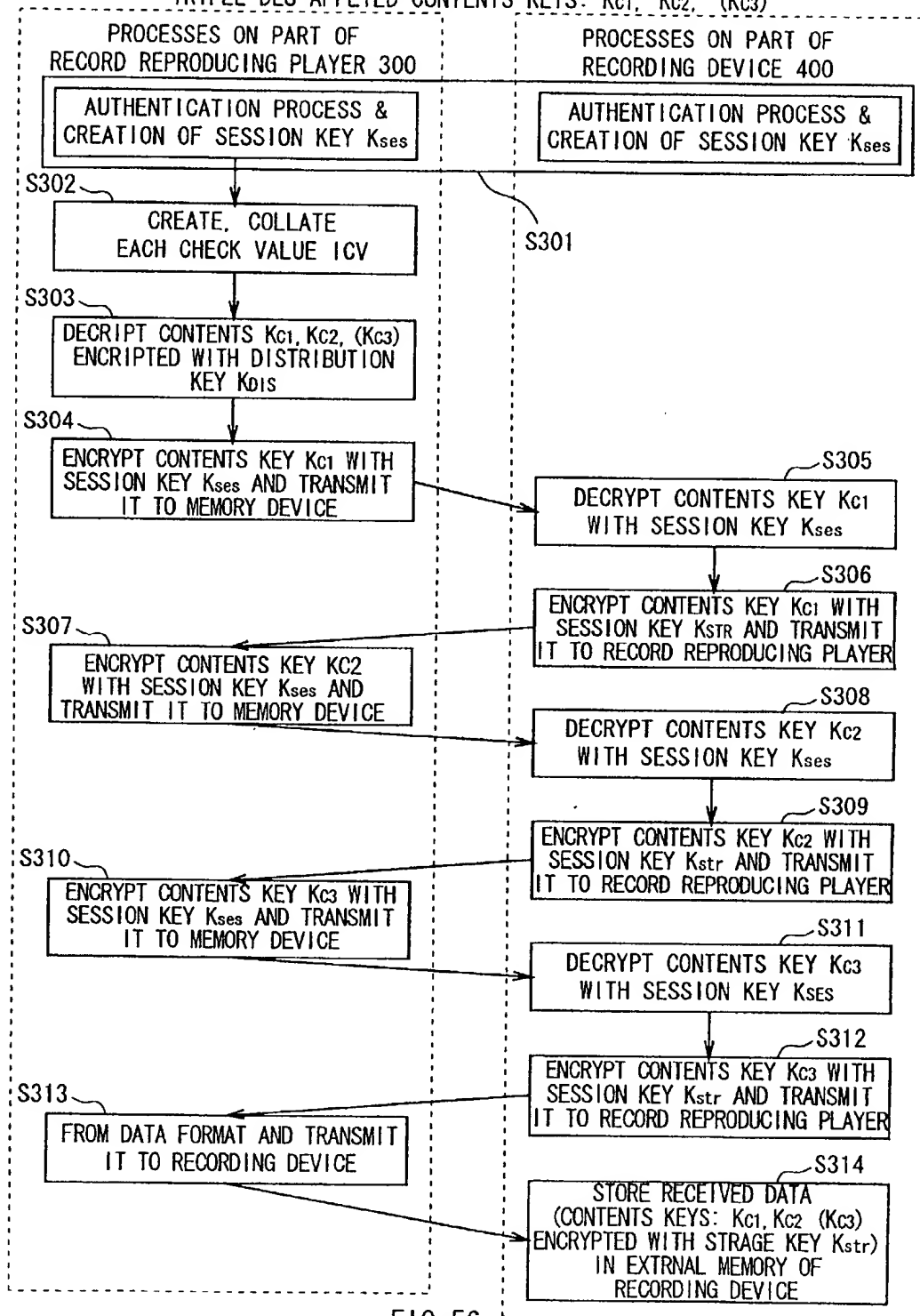


FIG. 56

09937410-121701

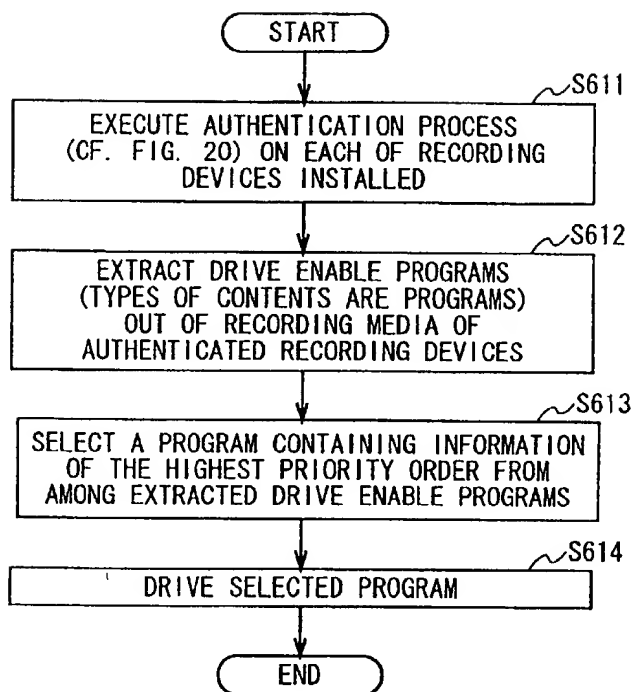


FIG. 57

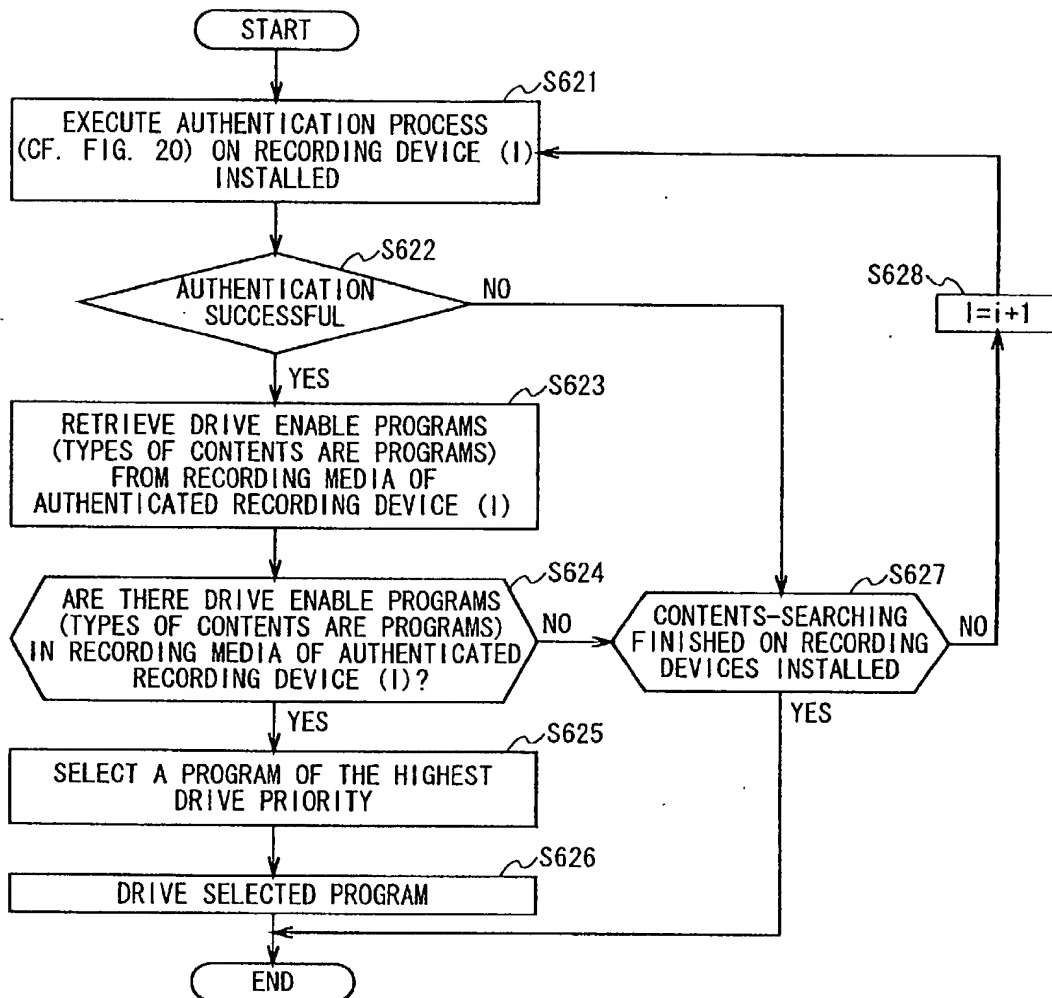


FIG. 58

09937410-121704

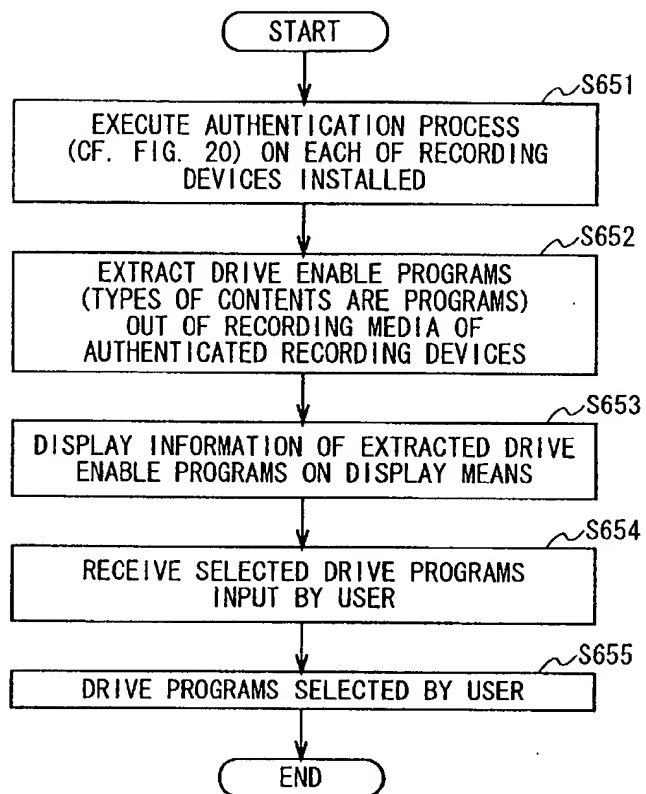


FIG. 59

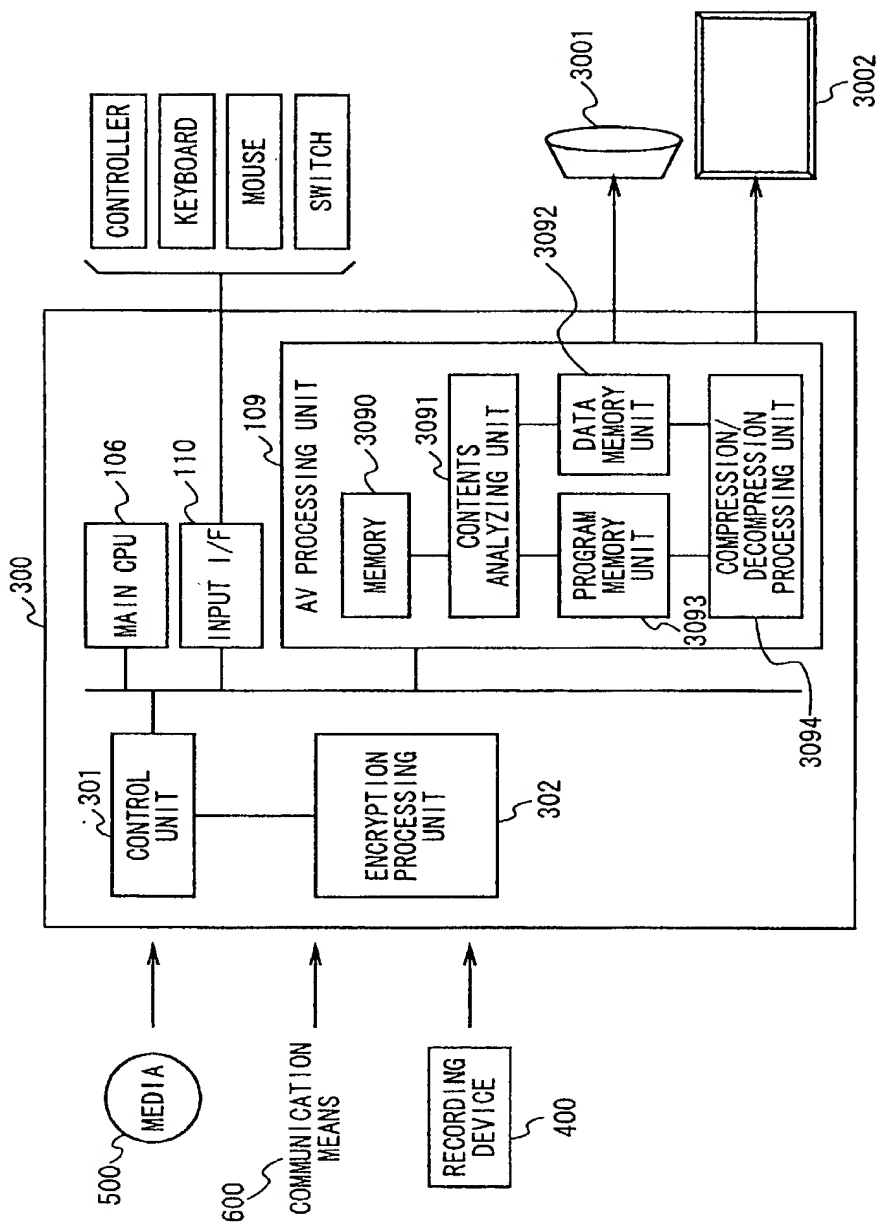


FIG. 60

EXAMPLE OF CONTENTS COMPOSITION (1)

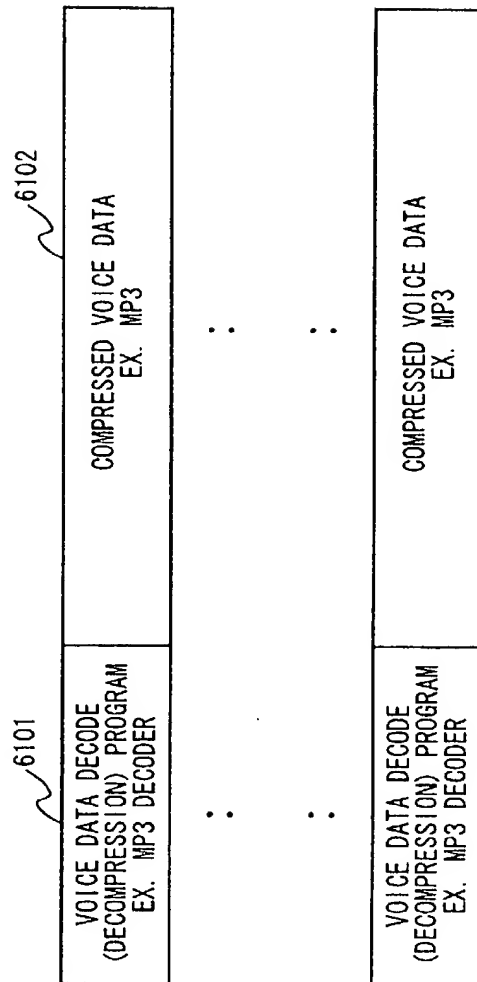


FIG. 61

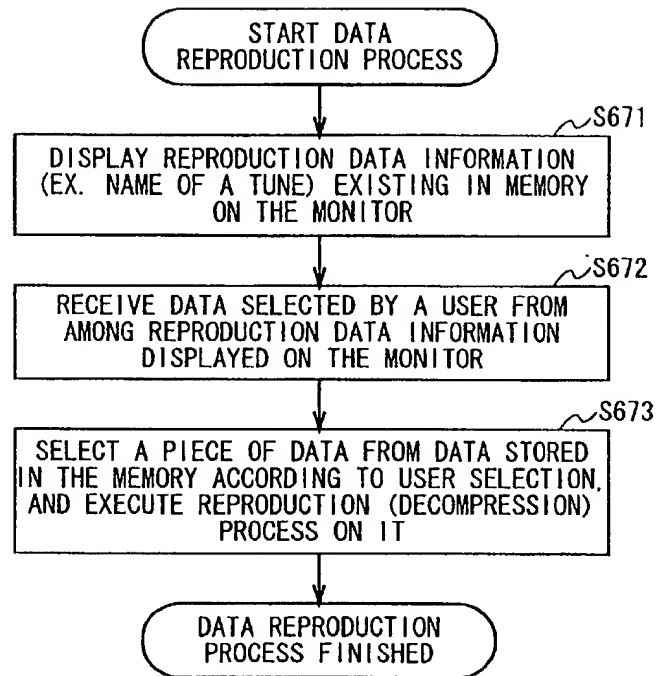


FIG. 62

FOOTNOTES

EXAMPLE OF CONTENTS COMPOSITION (2)

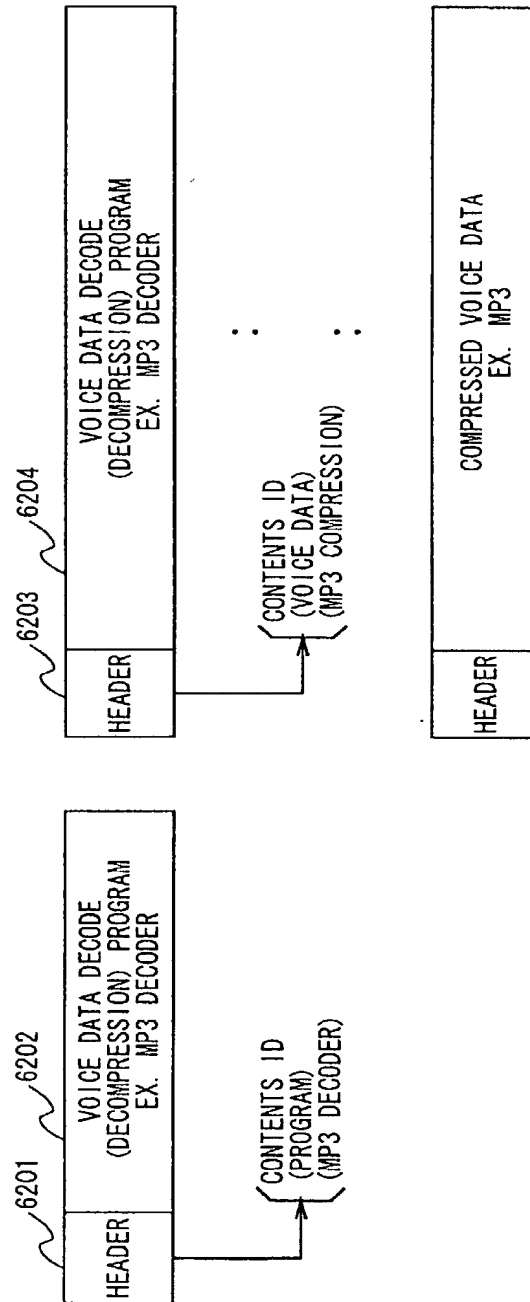


FIG. 63

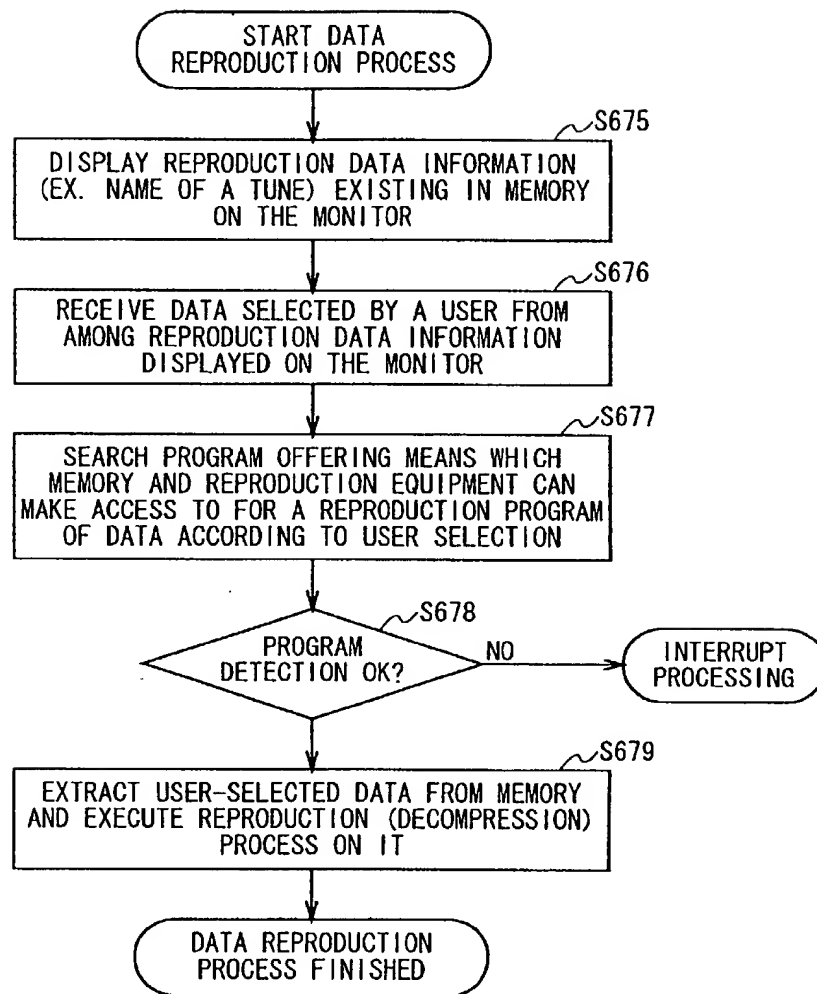


FIG. 64

FIG. 65

EXAMPLE OF CONTENTS COMPOSITION (3)

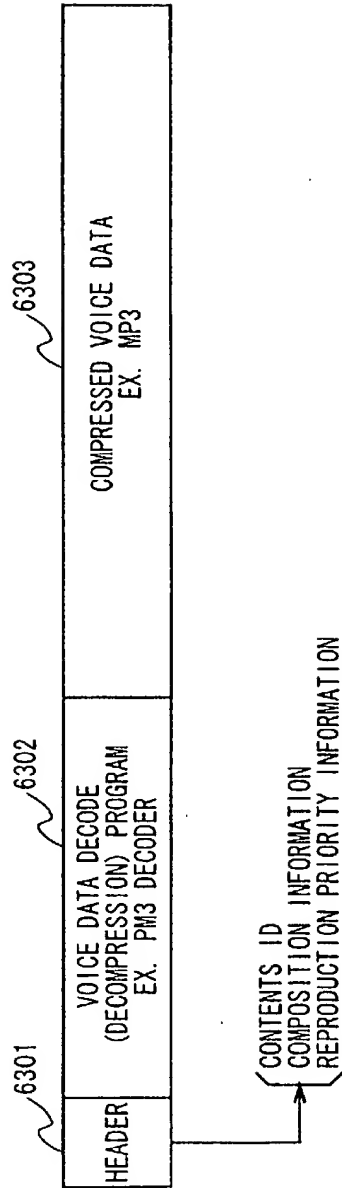


FIG. 65

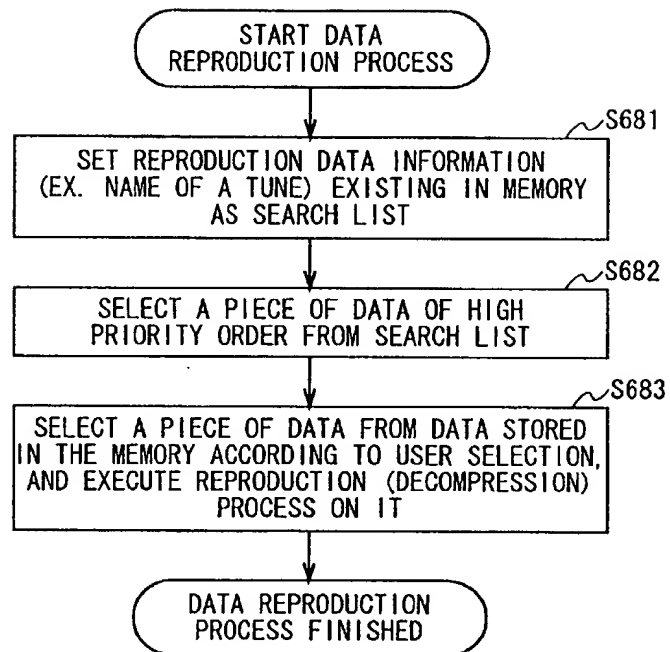


FIG. 66

EXAMPLE OF CONTENTS COMPOSITION (4)

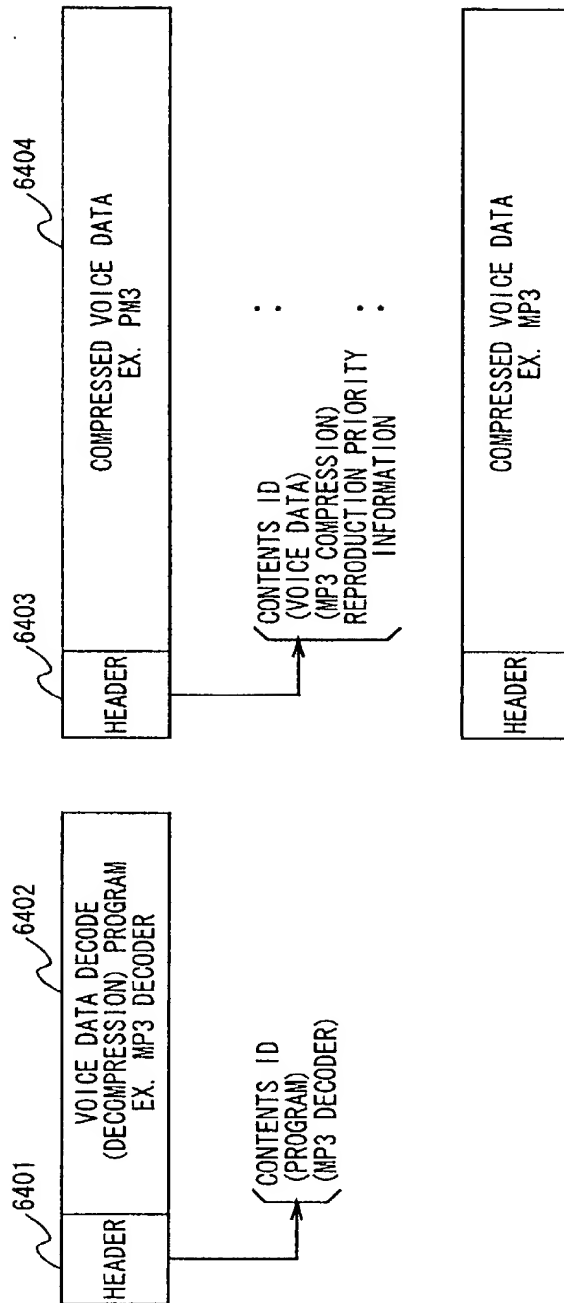


FIG. 67

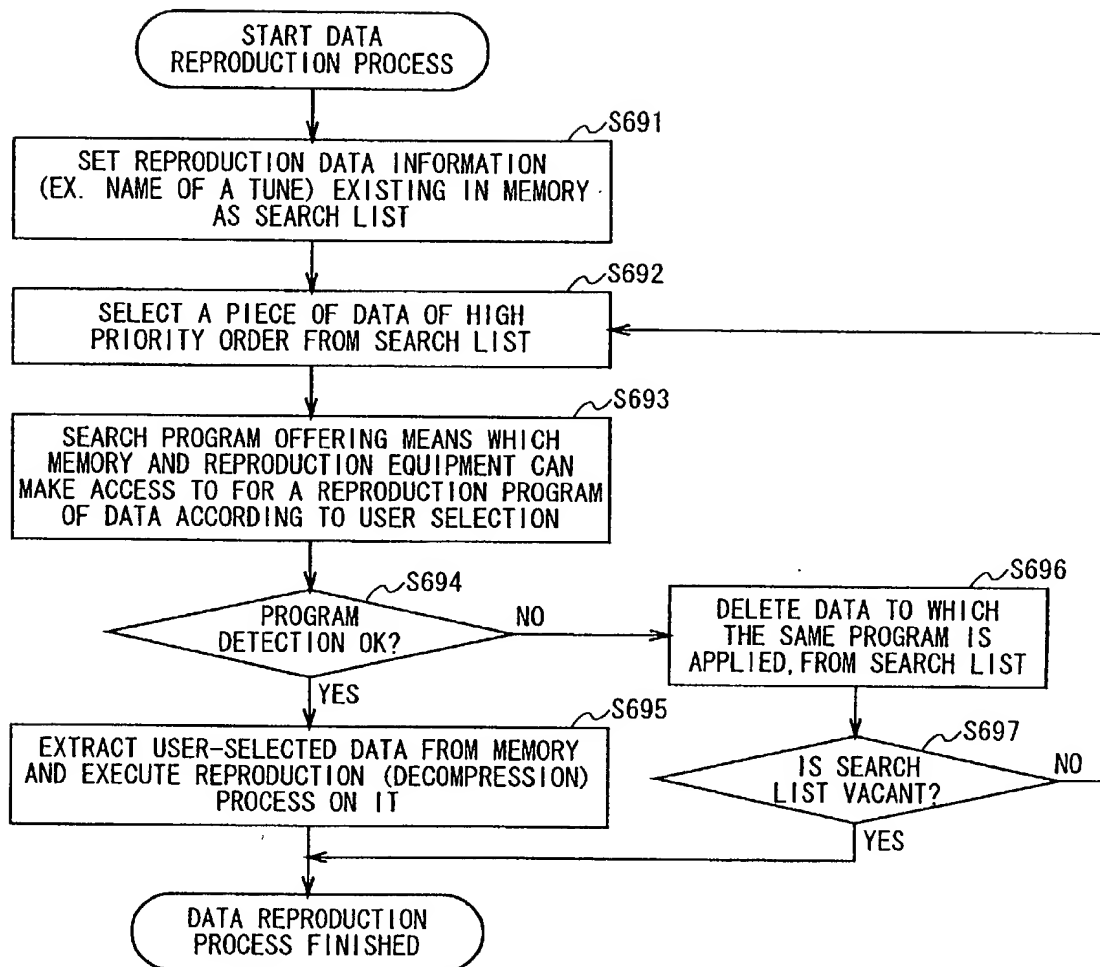
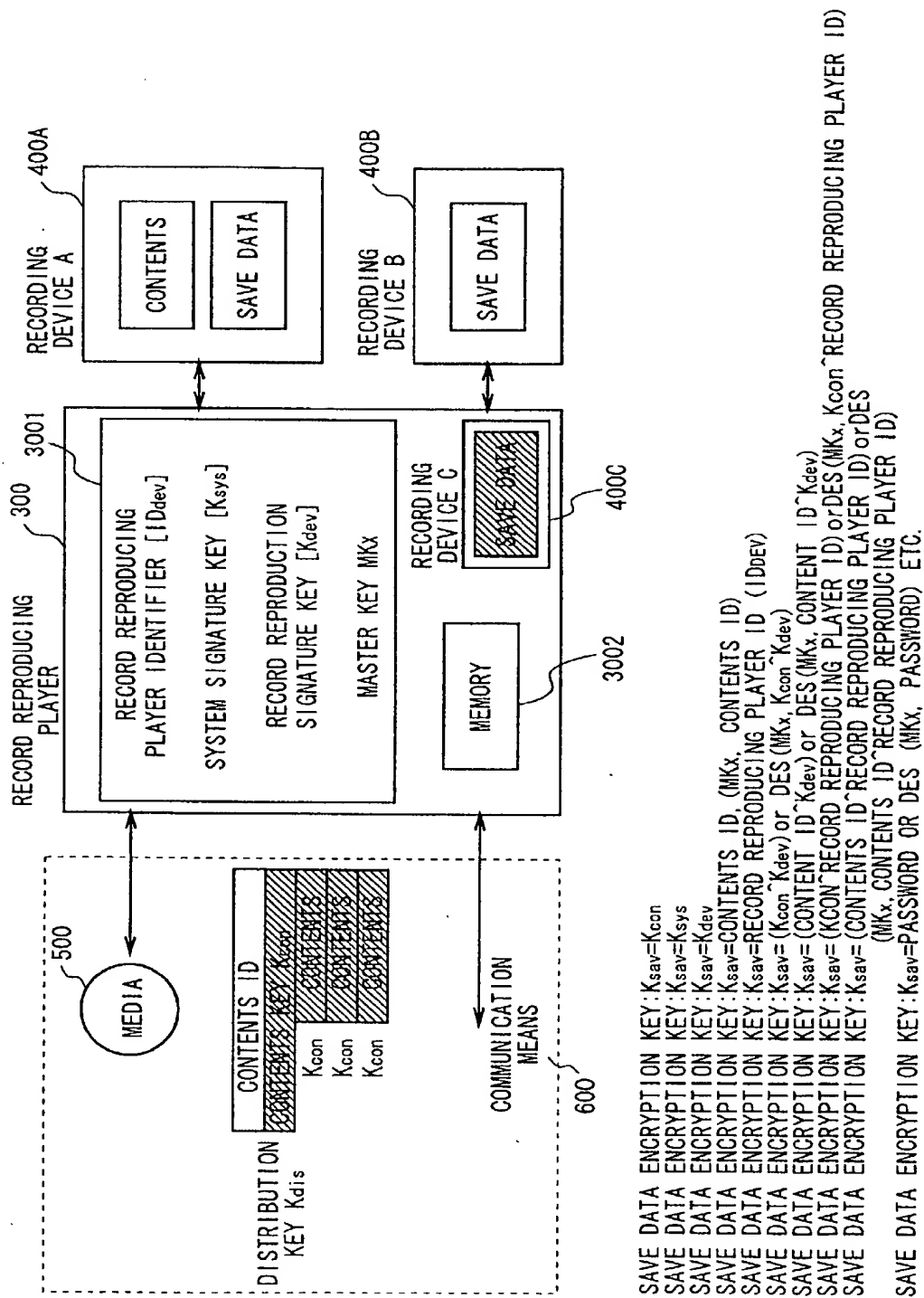


FIG. 68



**FIG. 69**

(1) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENTS INDIVIDUAL KEY, OR SYSTEM SHARED KEY

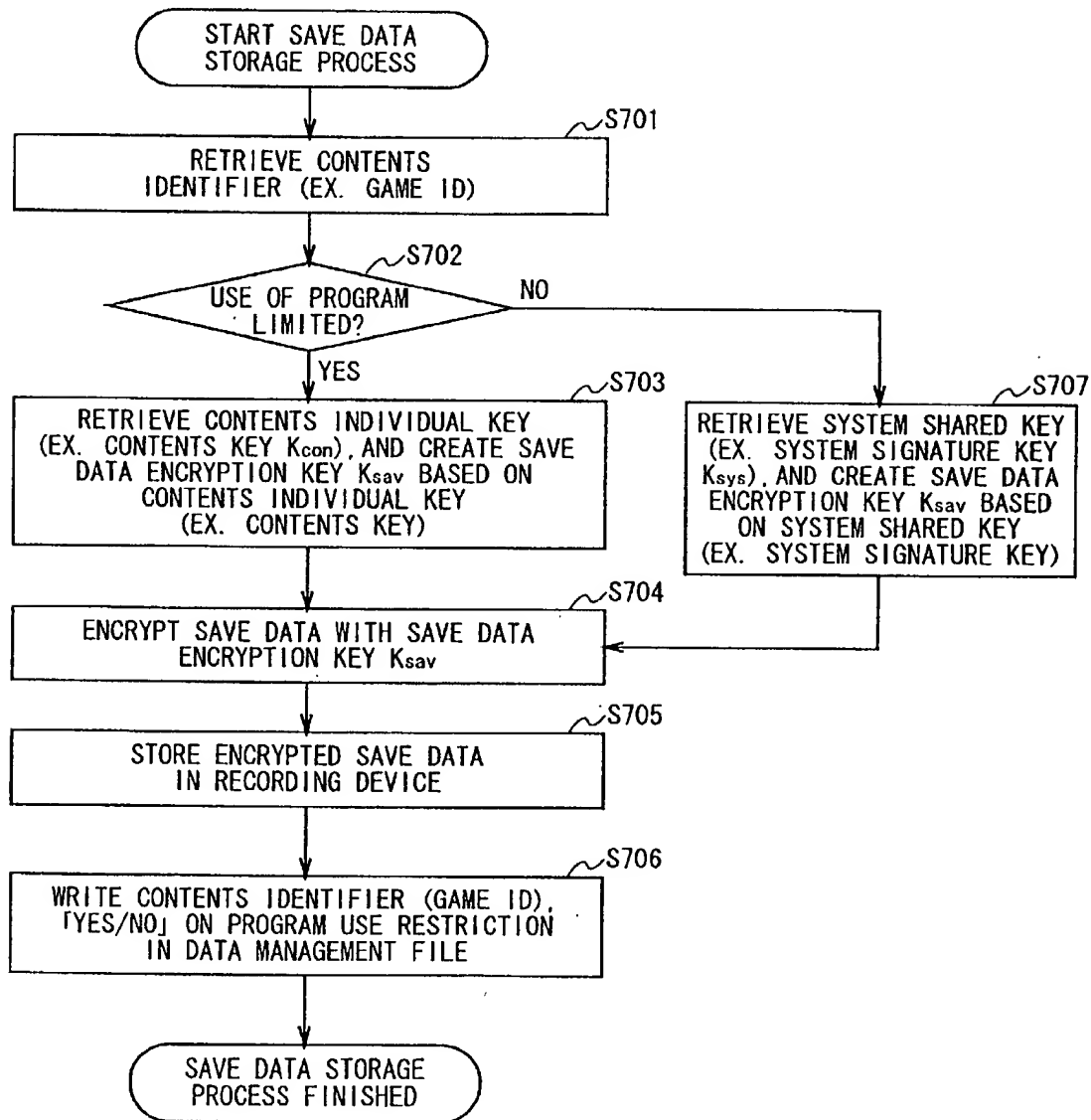


FIG. 70

FOUO 0144E660

DATA MANAGEMENT FILE (1)

DATA NO.	CONTENTS IDENTIFIER (GAME ID)	RECORD REPRODUCING PLAYER IDENTIFIER (ID <sub>dev</sub> )	PROGRAM USE RESTRICTION
1	12345678...	56789012...	YES
2	ABCDEF12...	09876543...	YES
3	12245678...	58834762...	NO
:	:	:	:

FIG. 71

## (2) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENTS INDIVIDUAL KEY, OR SYSTEM SHARED KEY

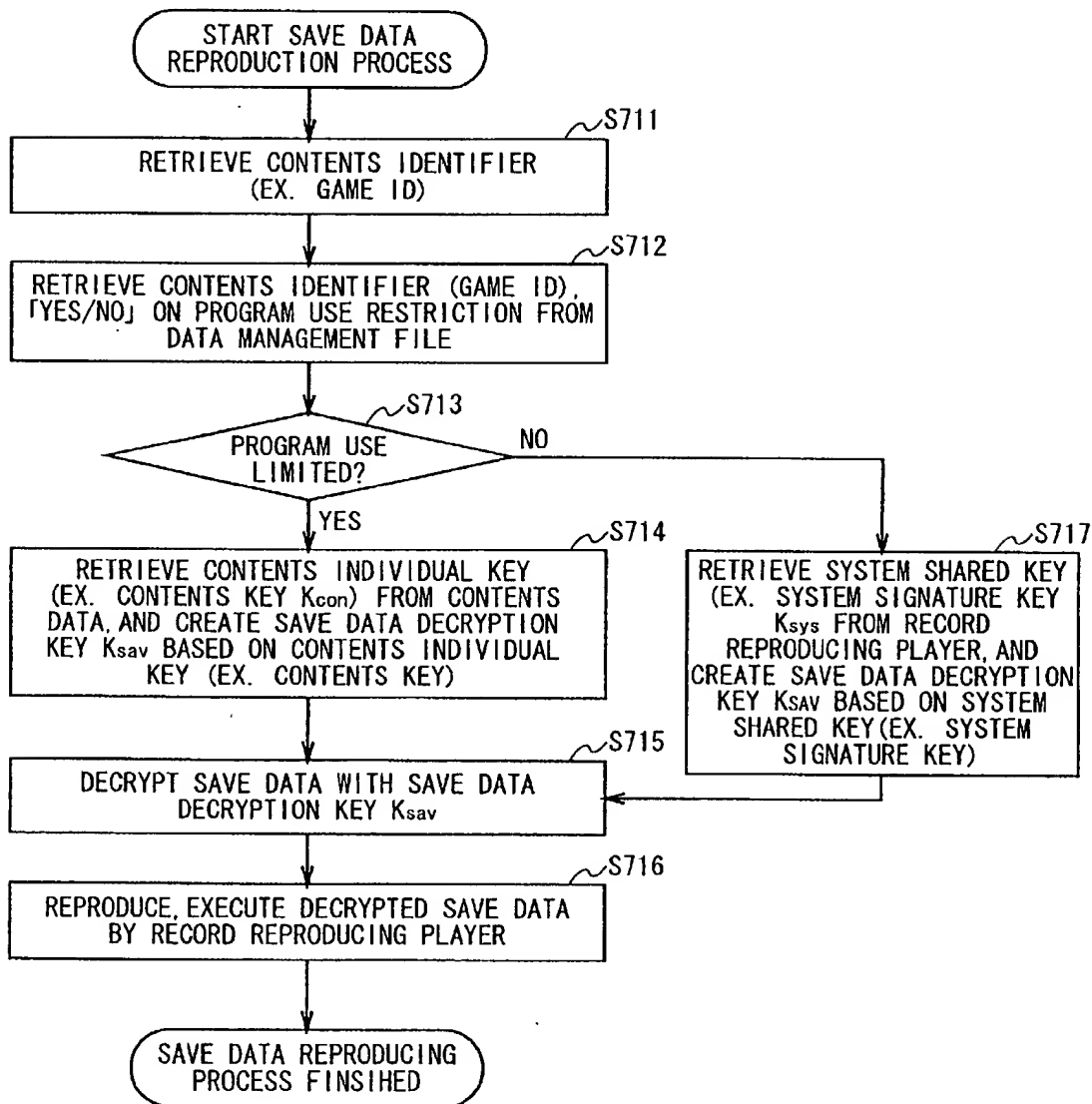


FIG. 72

## (3) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENTS ID, OR SYSTEM SHARED KEY

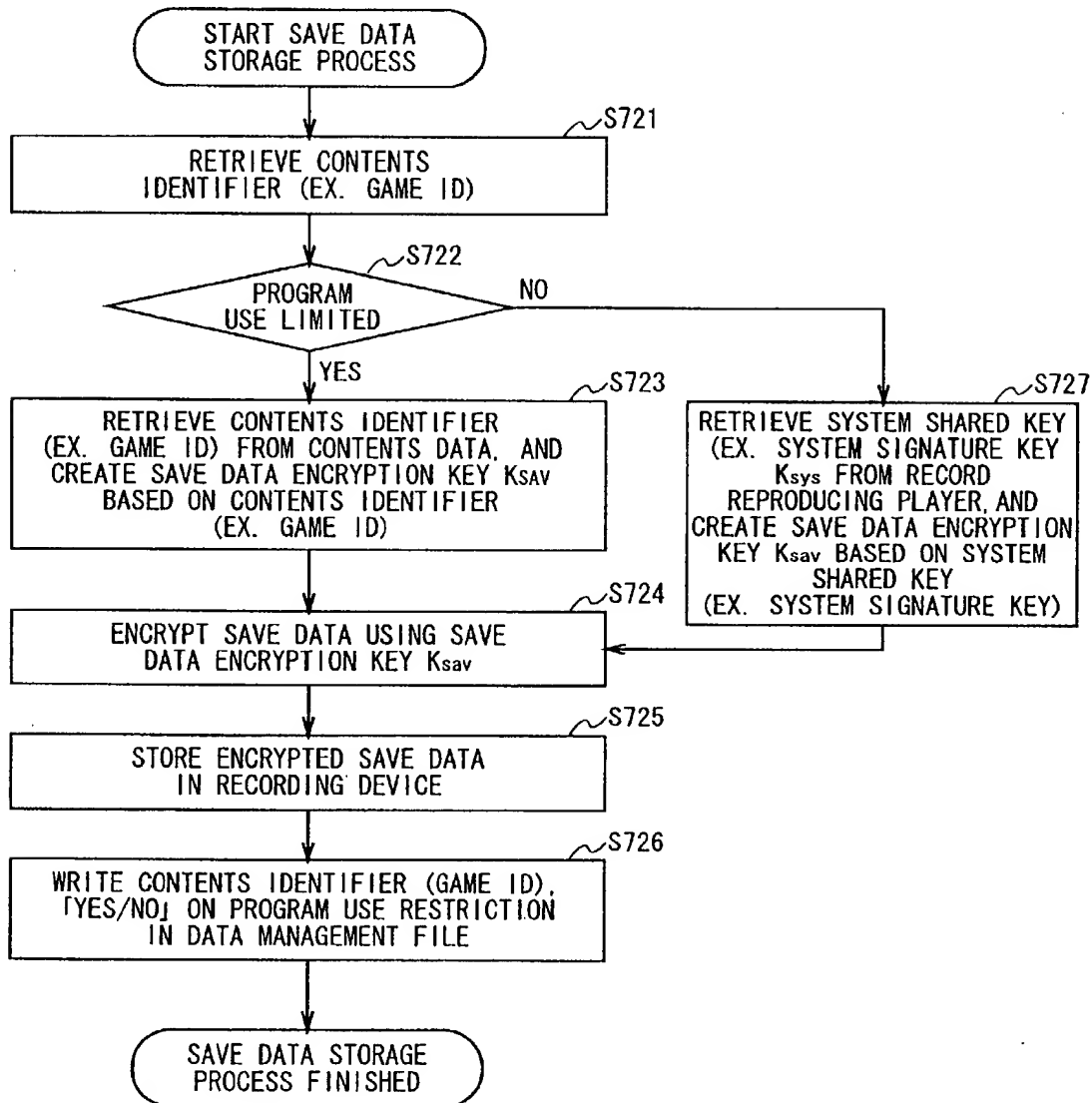


FIG. 73

(4) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENTS ID, OR SYSTEM SHARED KEY

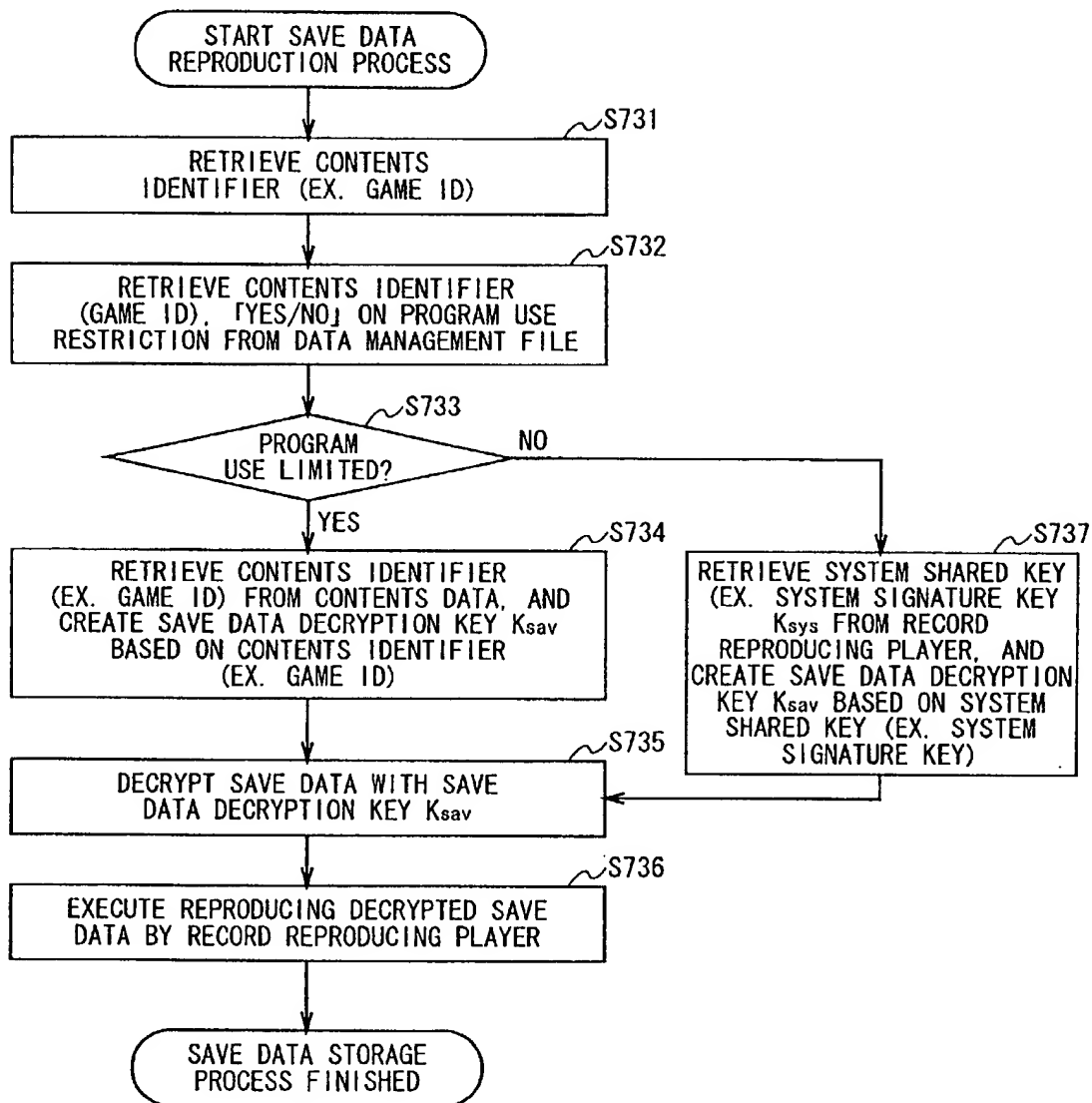


FIG. 74

(5) EXAMPLE OF SAVE DATA STORAGE PROCESS USING RECORD REPRODUCING  
PLAYER INDIVIDUAL KEY, OR SYSTEM SHARED KEY

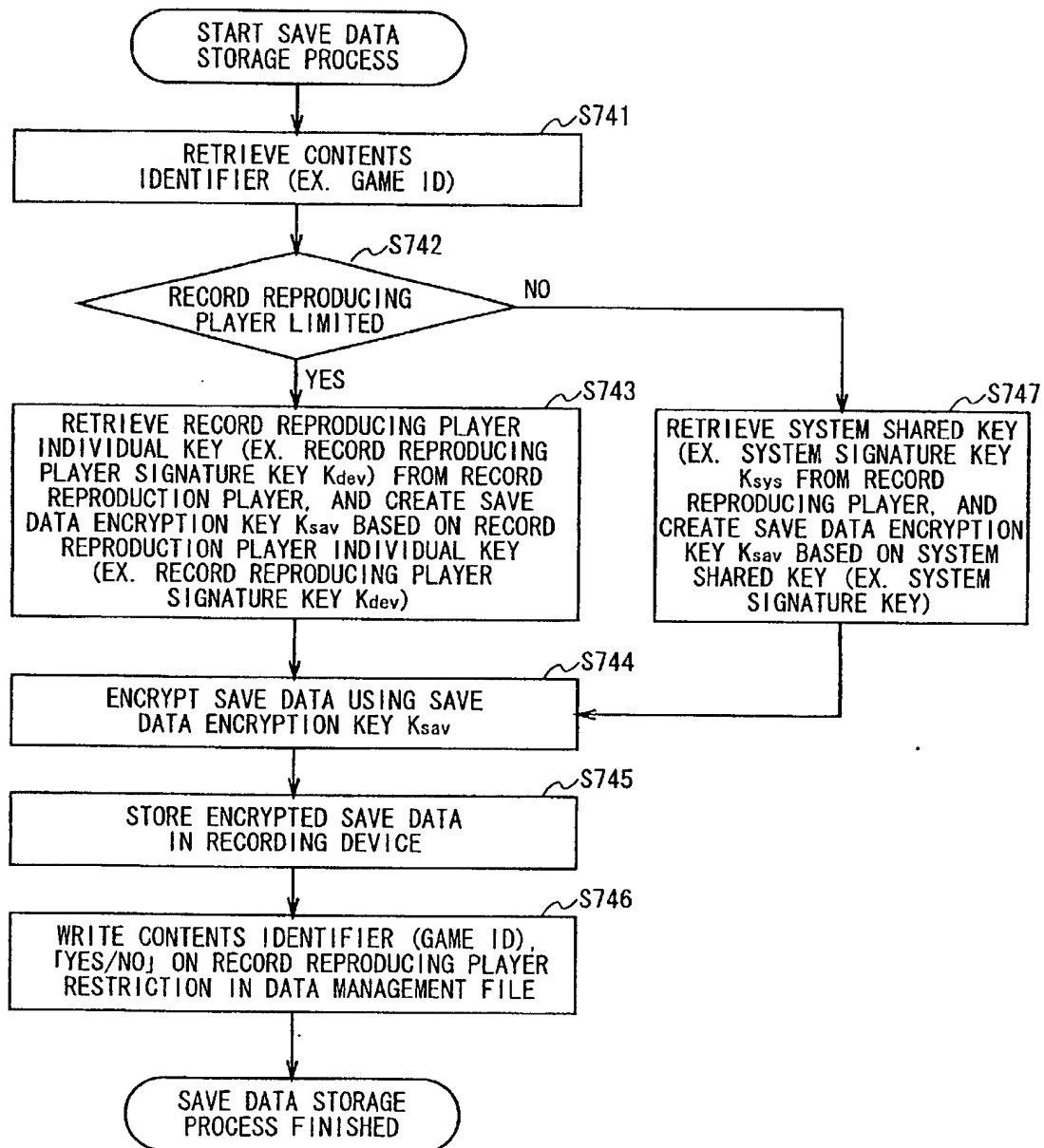


FIG. 75

10/2/2004 10:26:00

DATA MANAGEMENT FILE (2)

DATA NO.	CONTENTS IDENTIFIER (GAME ID)	RECORD REPRODUCING PLAYER IDENTIFIER (ID <sub>dev</sub> )	RECORD REPRODUCING PLAYER RESTRICTION
1	12345678...	56789012...	NO
2	ABCDEF12...	09876543...	YES
3	12245678...	58834762...	YES
...	...	...	...

FIG. 76

(6) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING RECORD  
REPRODUCING PLAYER INDIVIDUAL KEY, OR SYSTEM SHARED KEY

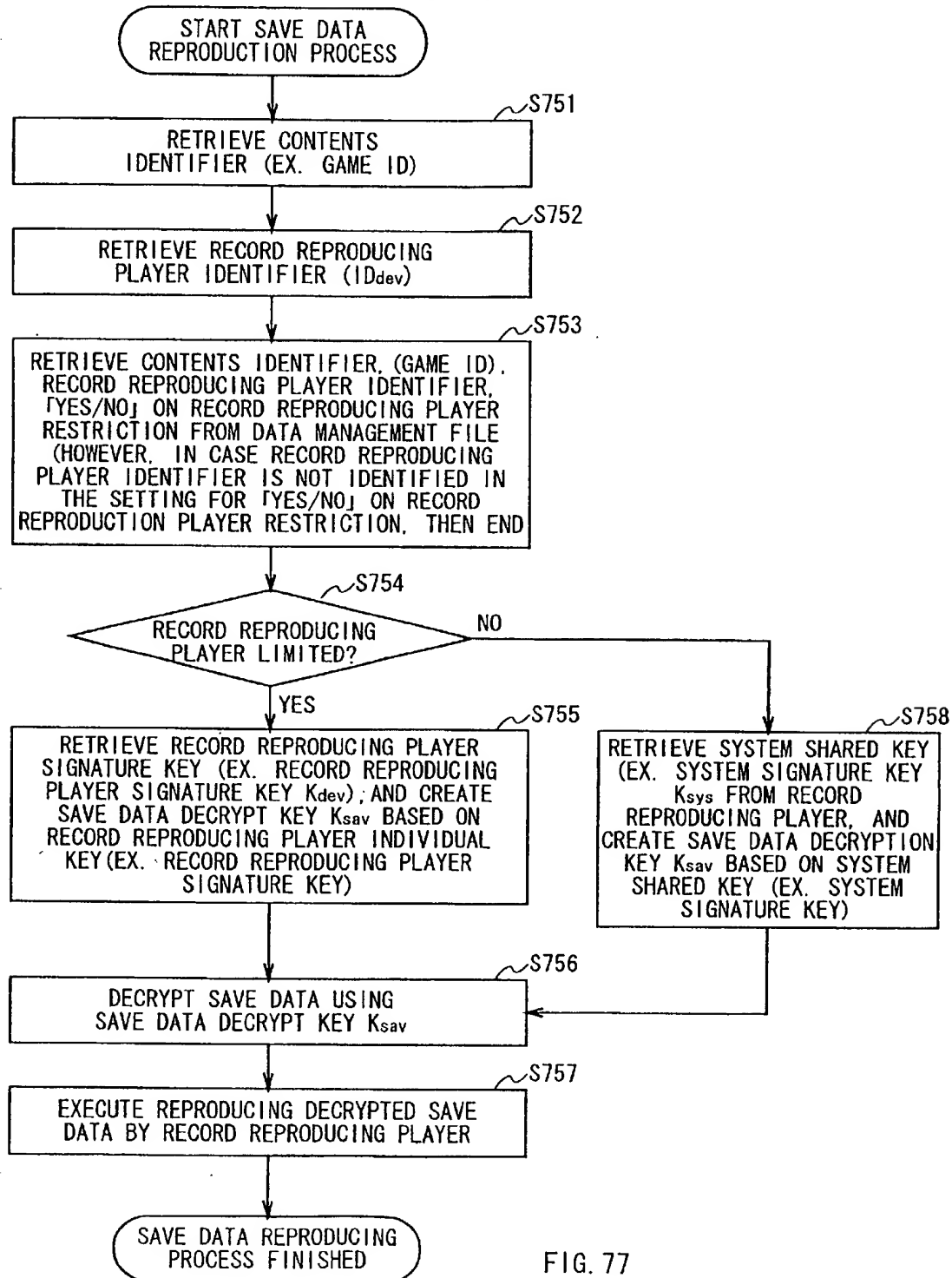


FIG. 77

(7) EXAMPLE OF SAVE DATA STORAGE PROCESS USING RECORD REPRODUCING PLAYER IDENTIFIER, OR SYSTEM SHARED KEY

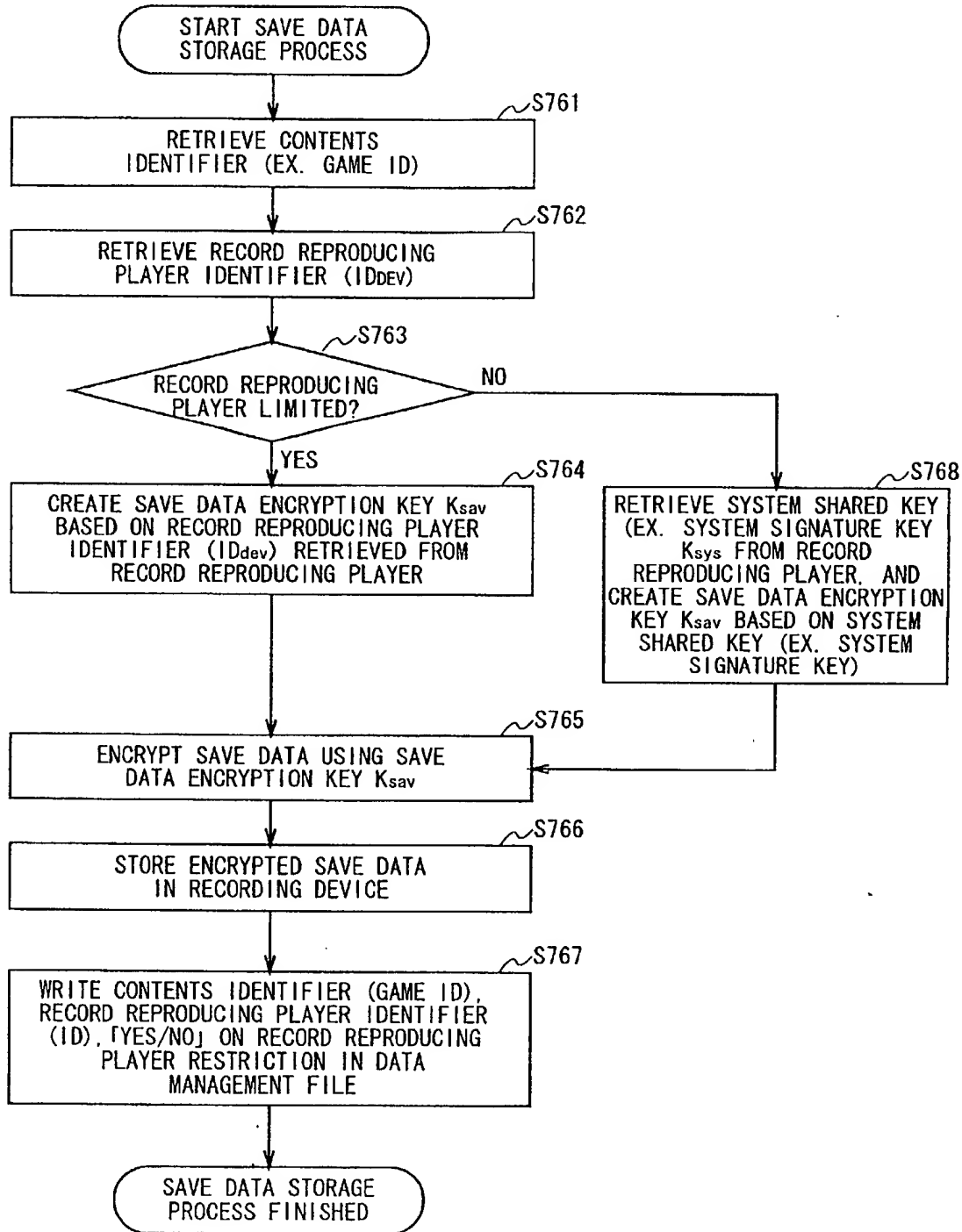


FIG. 78

## (8) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING RECORD REPRODUCING PLAYER IDENTIFIER, OR SYSTEM SHARED KEY

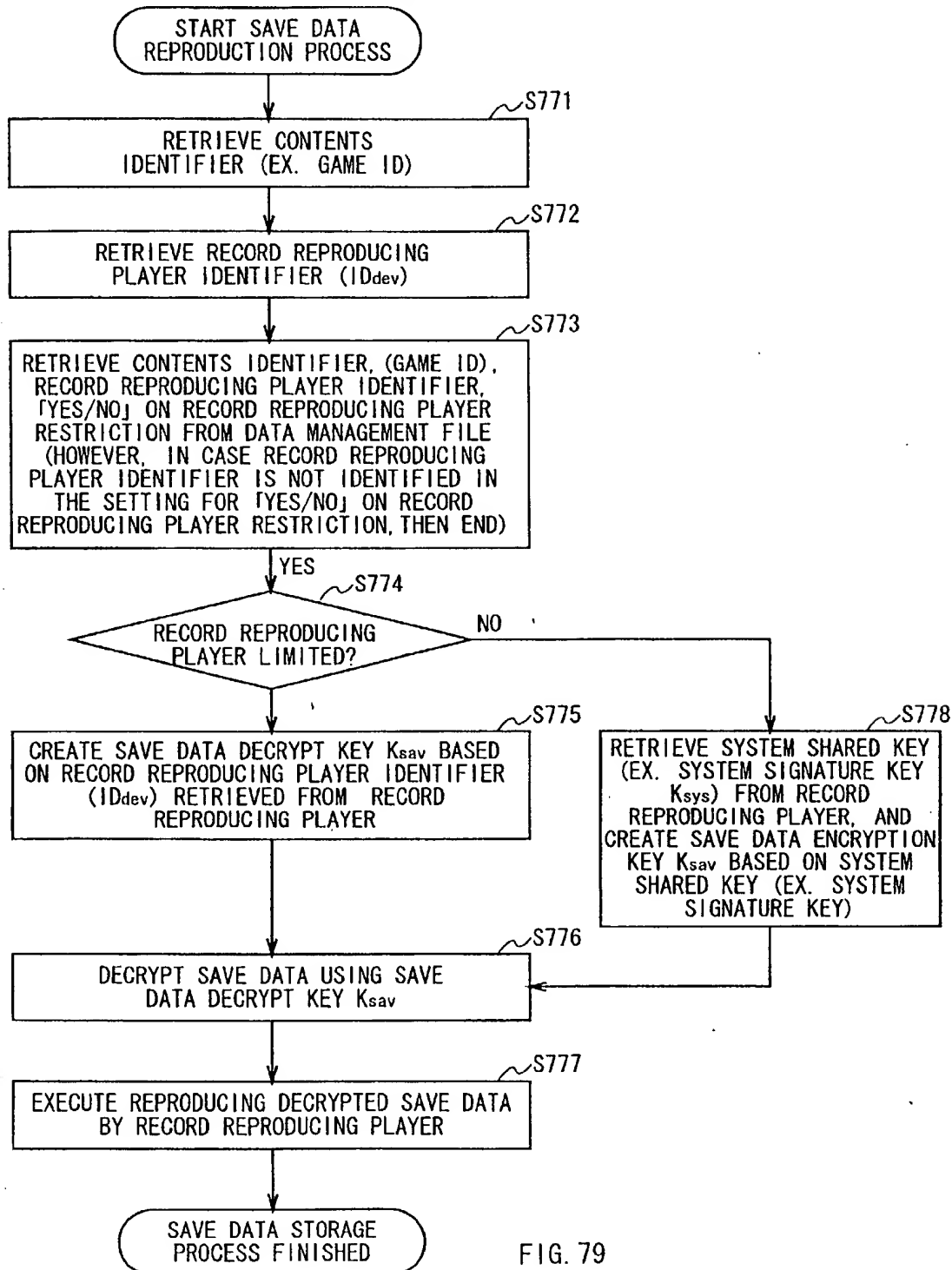


FIG. 79

FIG. 80

(9) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENTS INDIVIDUAL KEY, RECORD REPRODUCING PLAYER INDIVIDUAL KEY, OR SYSTEM SHARED KEY

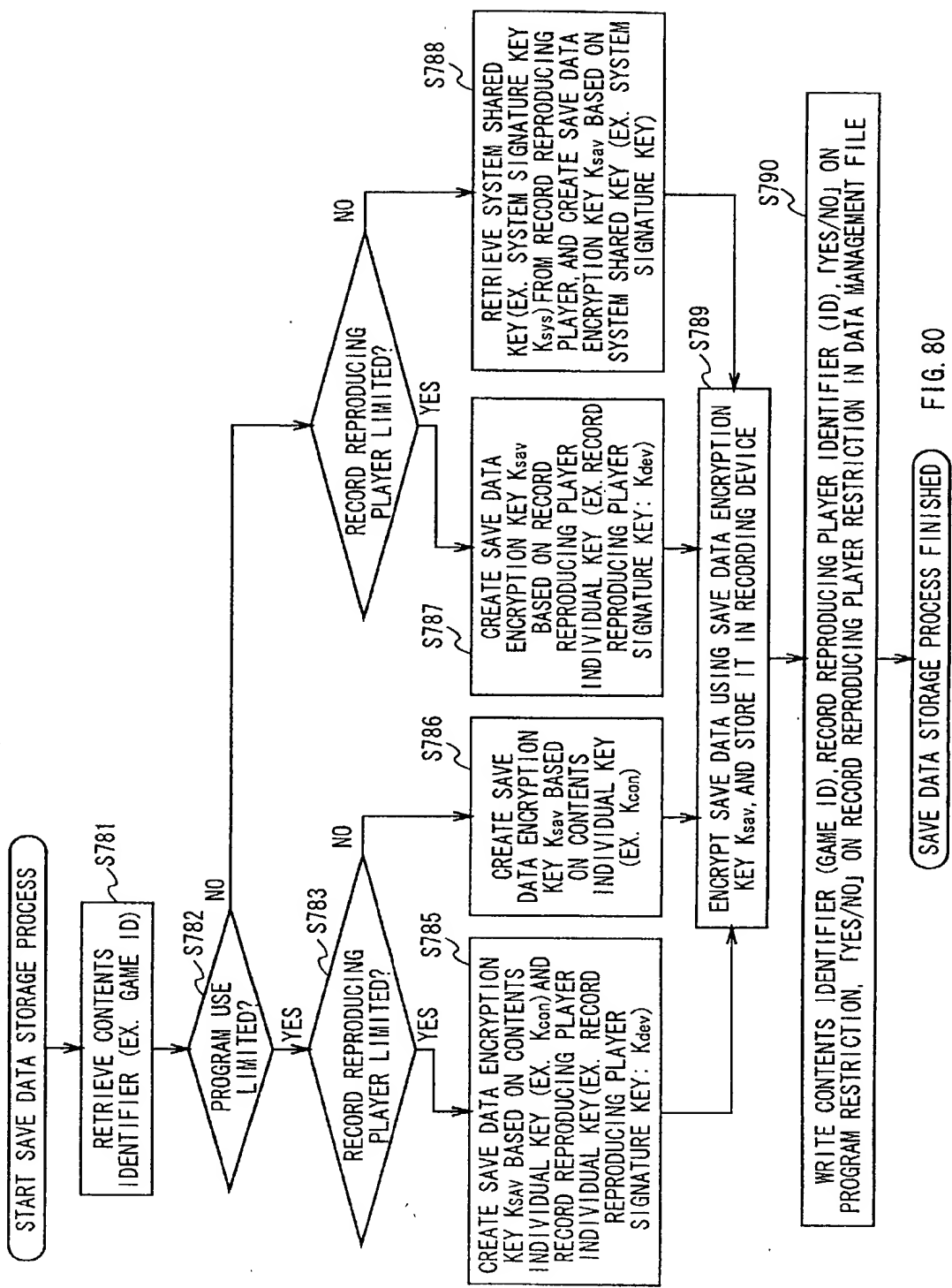


FIG. 80

DATA MANAGEMENT FILE (3)

DATA NO.	CONTENTS IDENTIFIER (GAME ID)	RECORD REPRODUCING PLAYER IDENTIFIER (IDdev)	PROGRAM USE RESTRICTION	RECORD REPRODUCING PLAYER RESTRICTION
1	123455678...	56789012...	YES	NO
2	ABCDEF12...	09876543...	YES	YES
3	1122457678	58834762...	NO	YES
...	...	...	...	...
...	...	...	...	...

FIG. 81

FIG. 82

(10) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENT UNIQUE KEY, RECORDING AND REPRODUCING DEVICE UNIQUE KEY, OR SYSTEM COMMON KEY

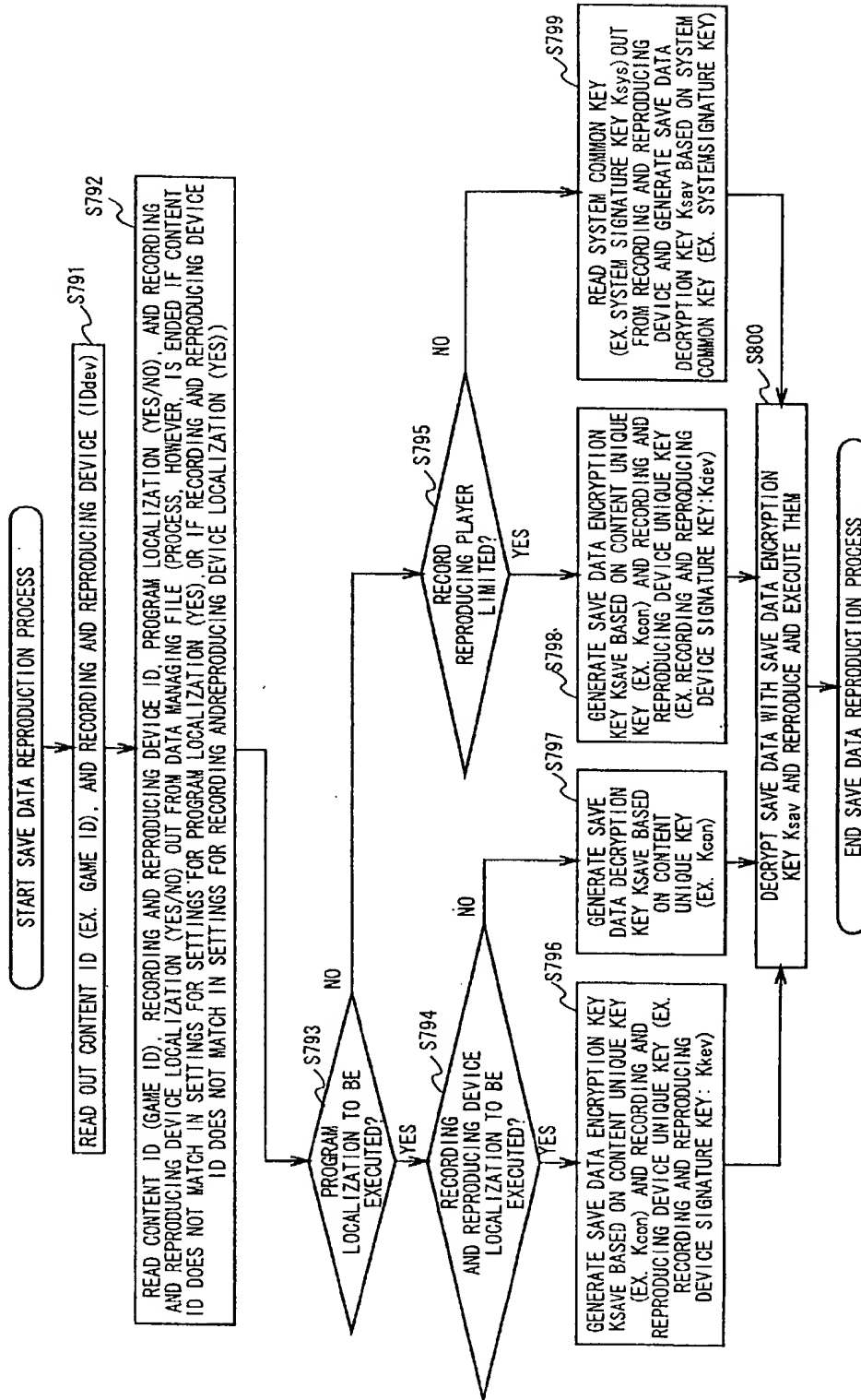


FIG. 82

(11) EXAMPLE OF SAVE DATA STORAGE PROCESS USING USER PASSWORD,  
OR SYSTEM SHARED KEY

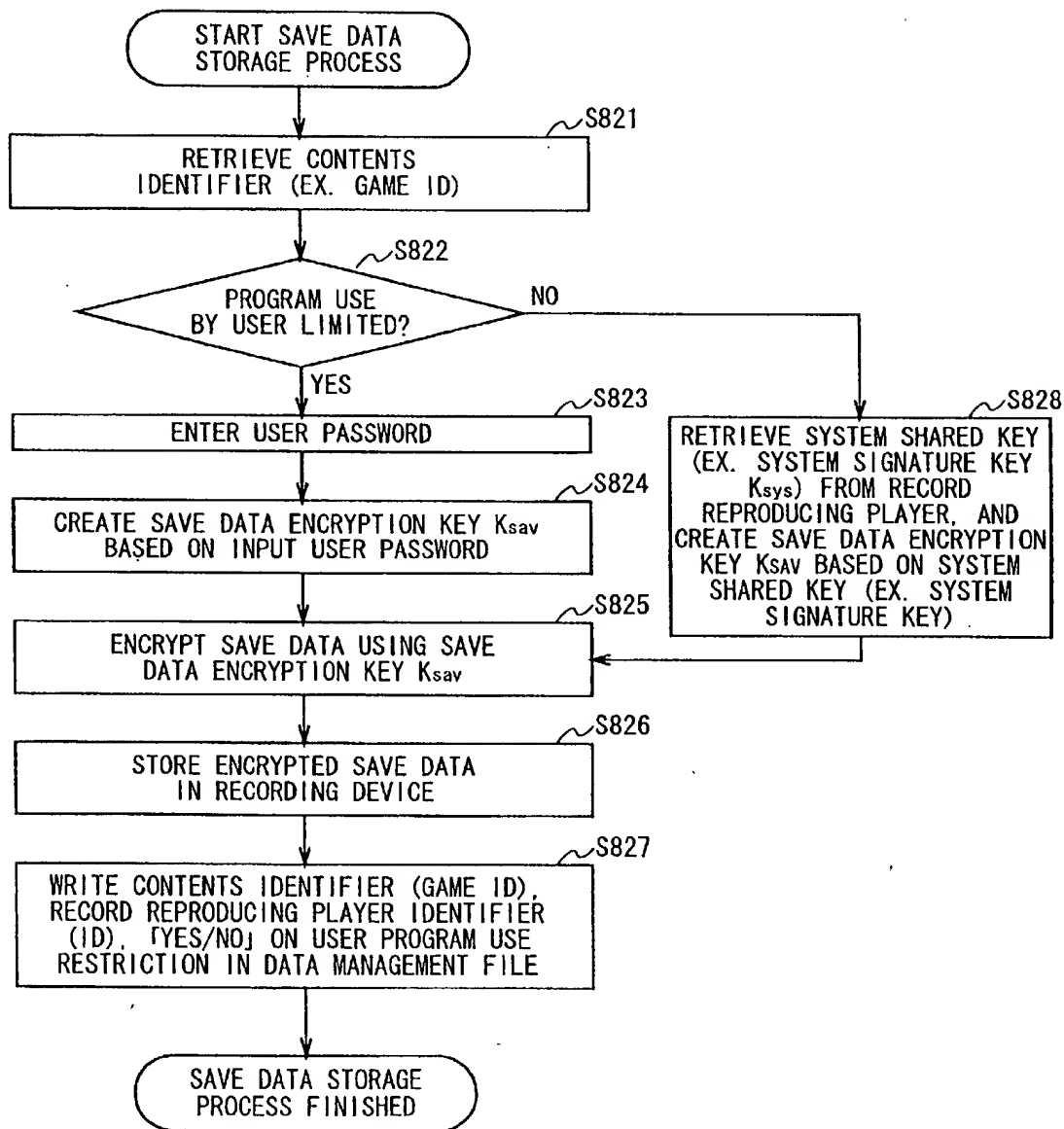


FIG. 83

FORMAT OF HES60

DATA MANAGEMENT FILE (4)

DATA NO.	CONTENTS IDENTIFIER (GAME ID)	RECORD REPRODUCING PLAYER IDENTIFIER (ID <sub>dev</sub> )	USER PROGRAM USE RESTRICTION
1	123455678...	56789012...	YES
2	ABCDEF12...	09876543...	YES
3	1122457678	58834762...	NO
•	•	•	•
•	•	•	•

FIG. 84

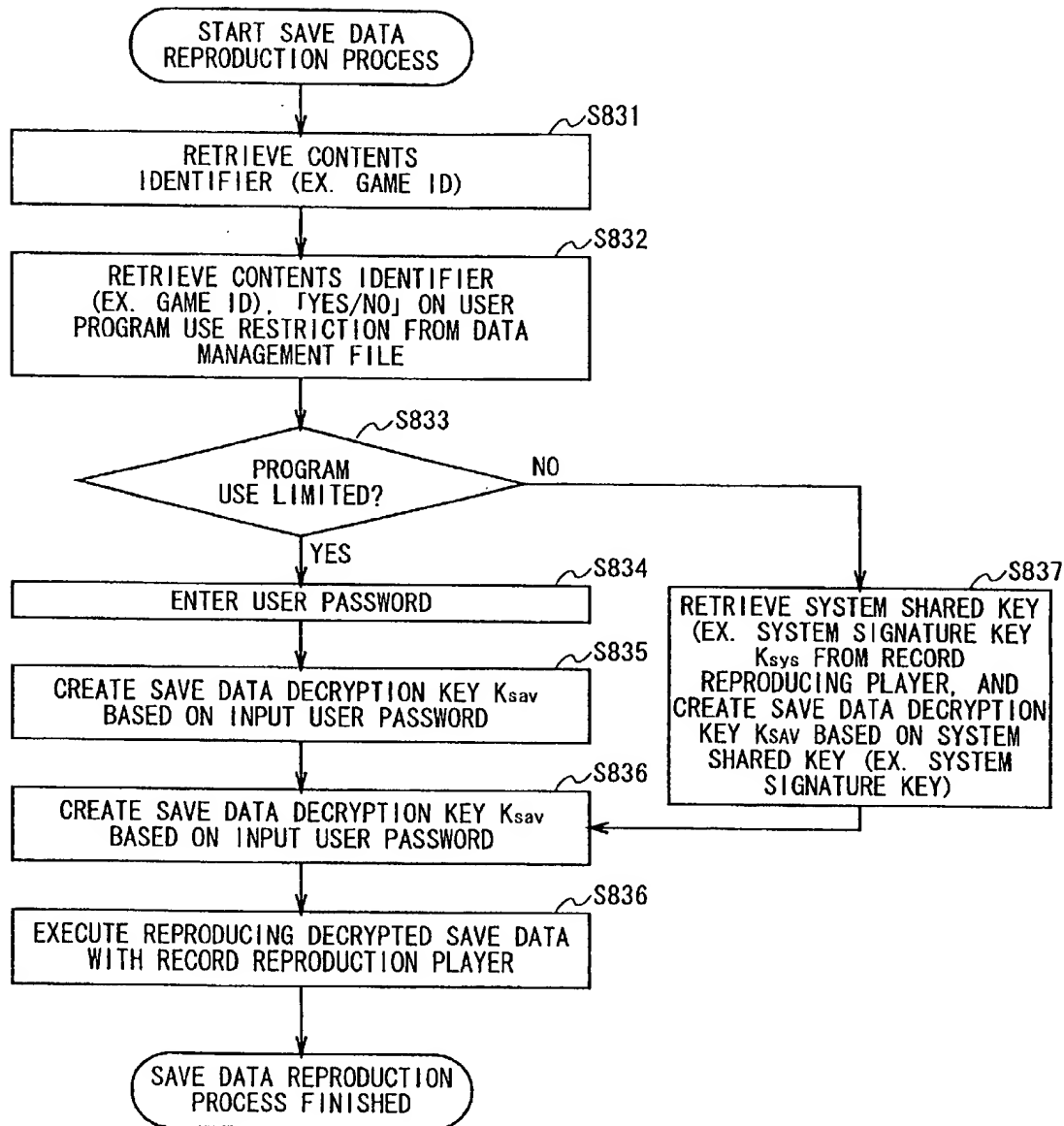
(12) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING USER PASSWORD,  
OR SYSTEM SHARED KEY

FIG. 85

FIG. 86

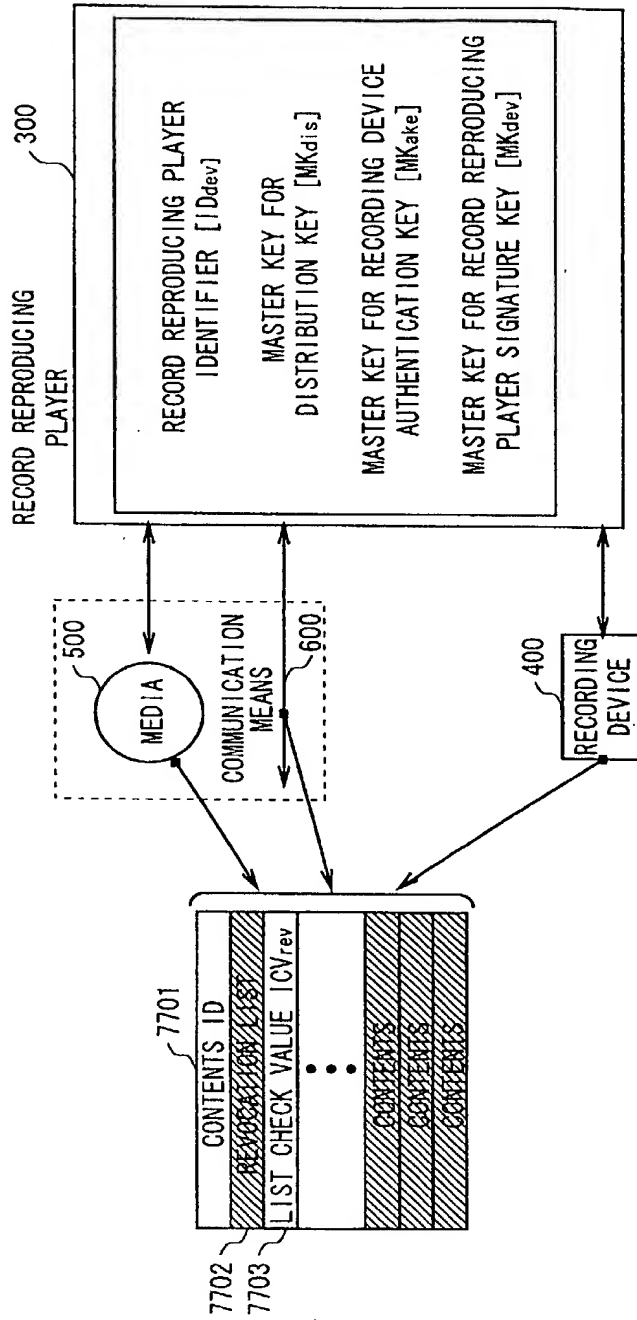


FIG. 86

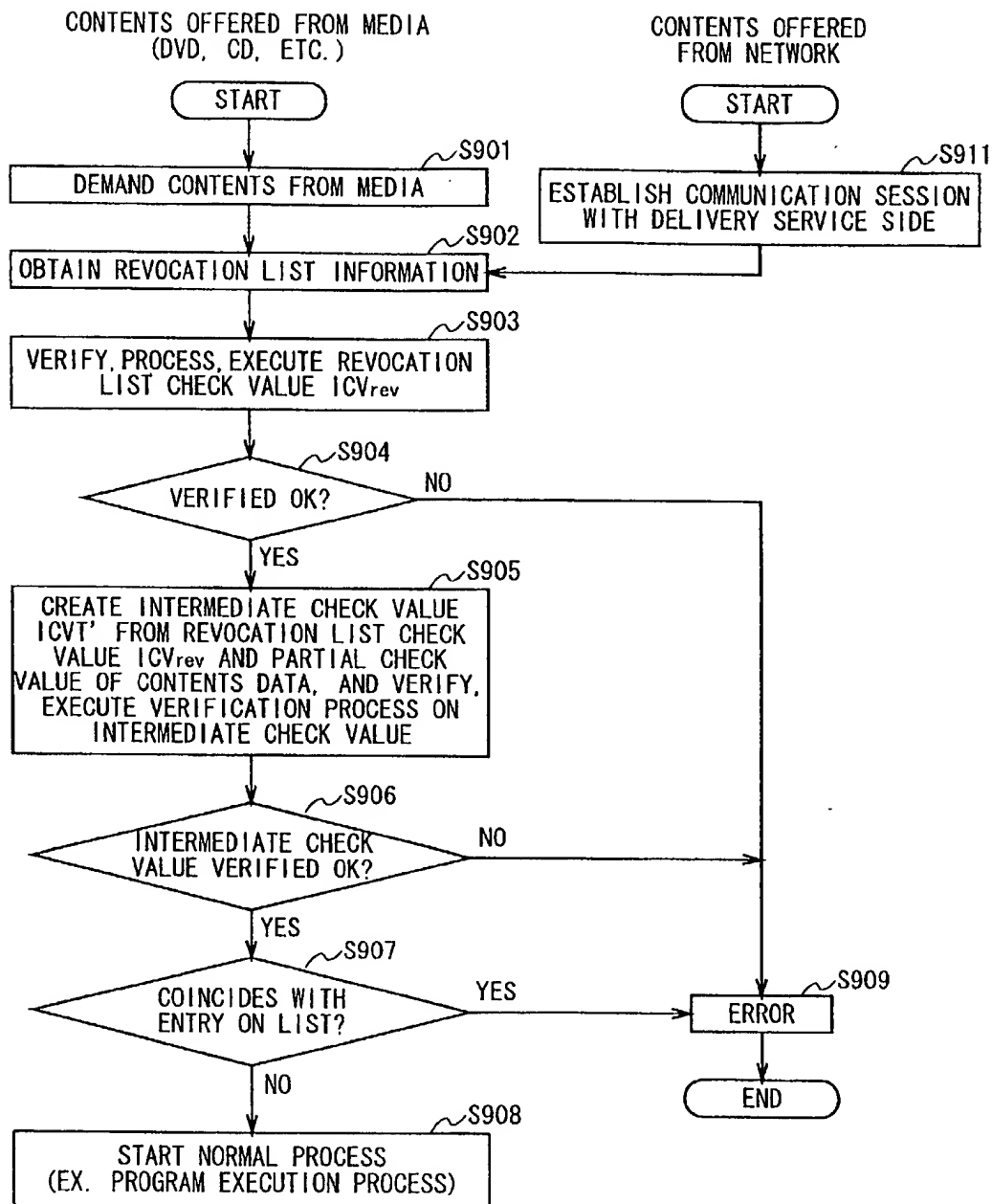


FIG. 87

CONTENTS OFFERED FROM RECORDING DEVICE  
(MEMORY CARD, ETC.)

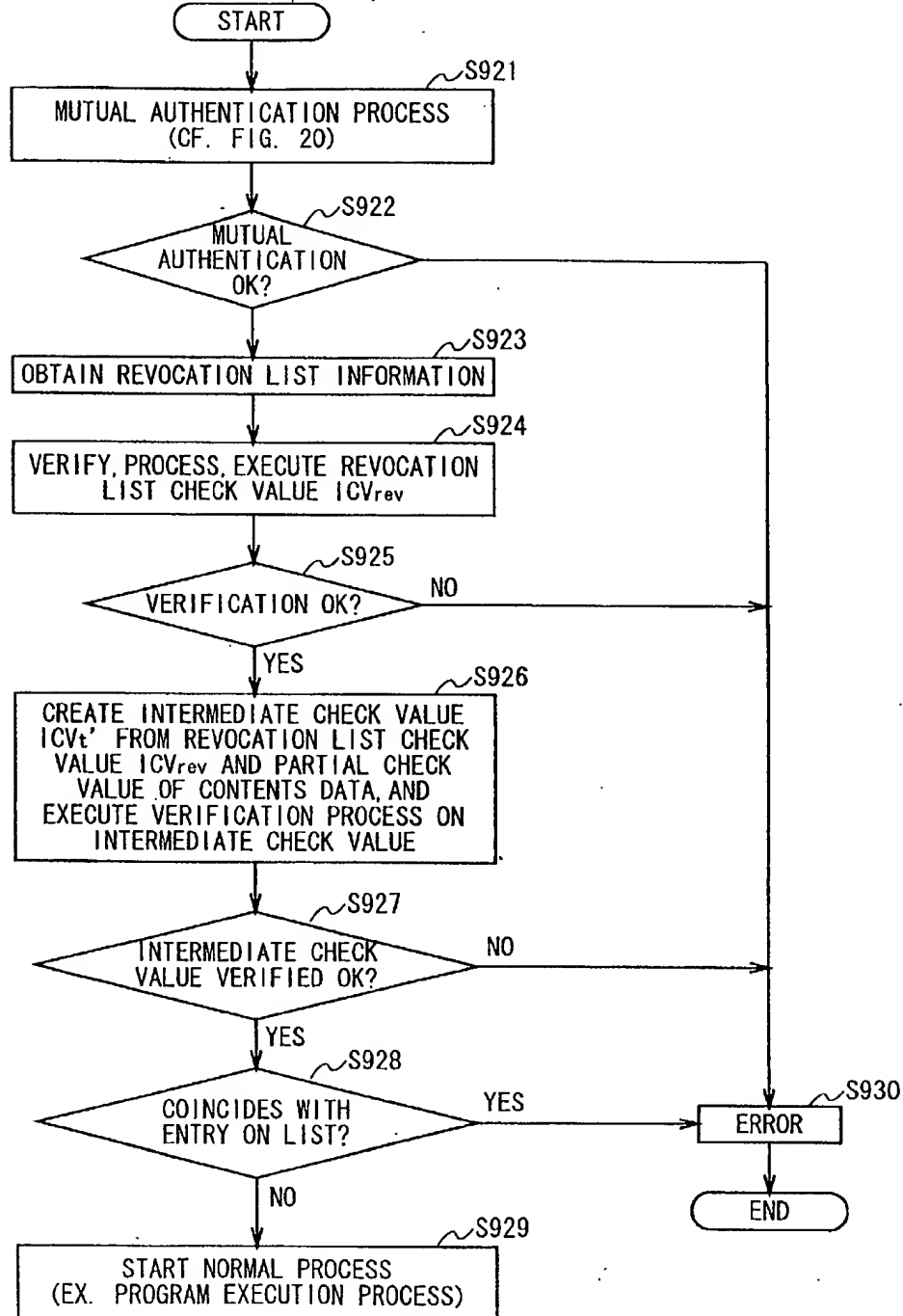


FIG. 88

87/93

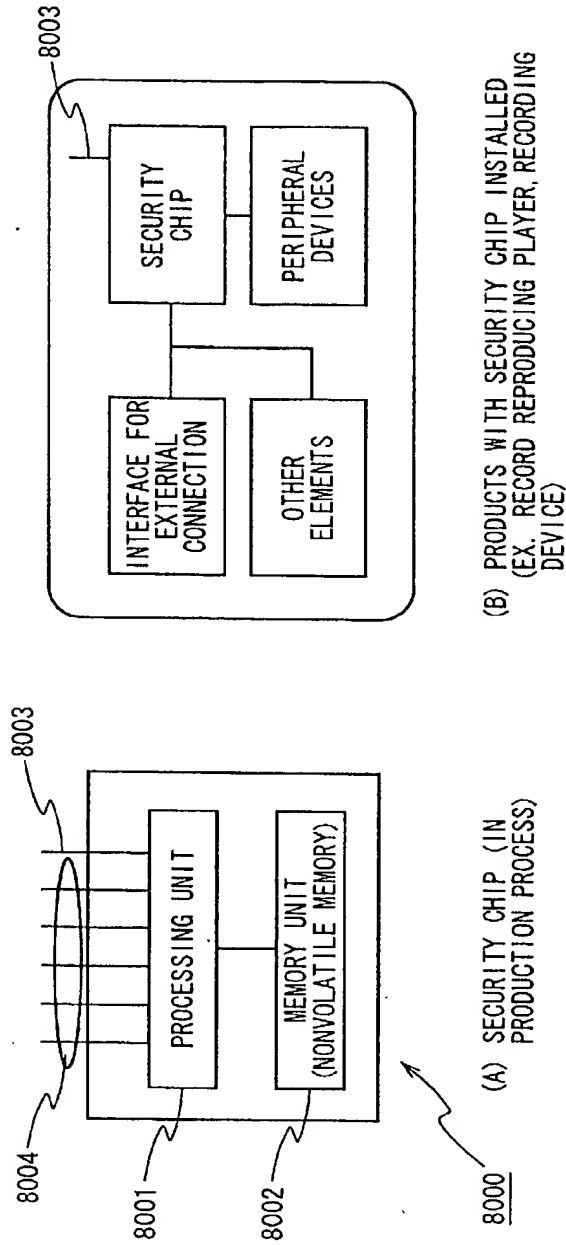


FIG. 89

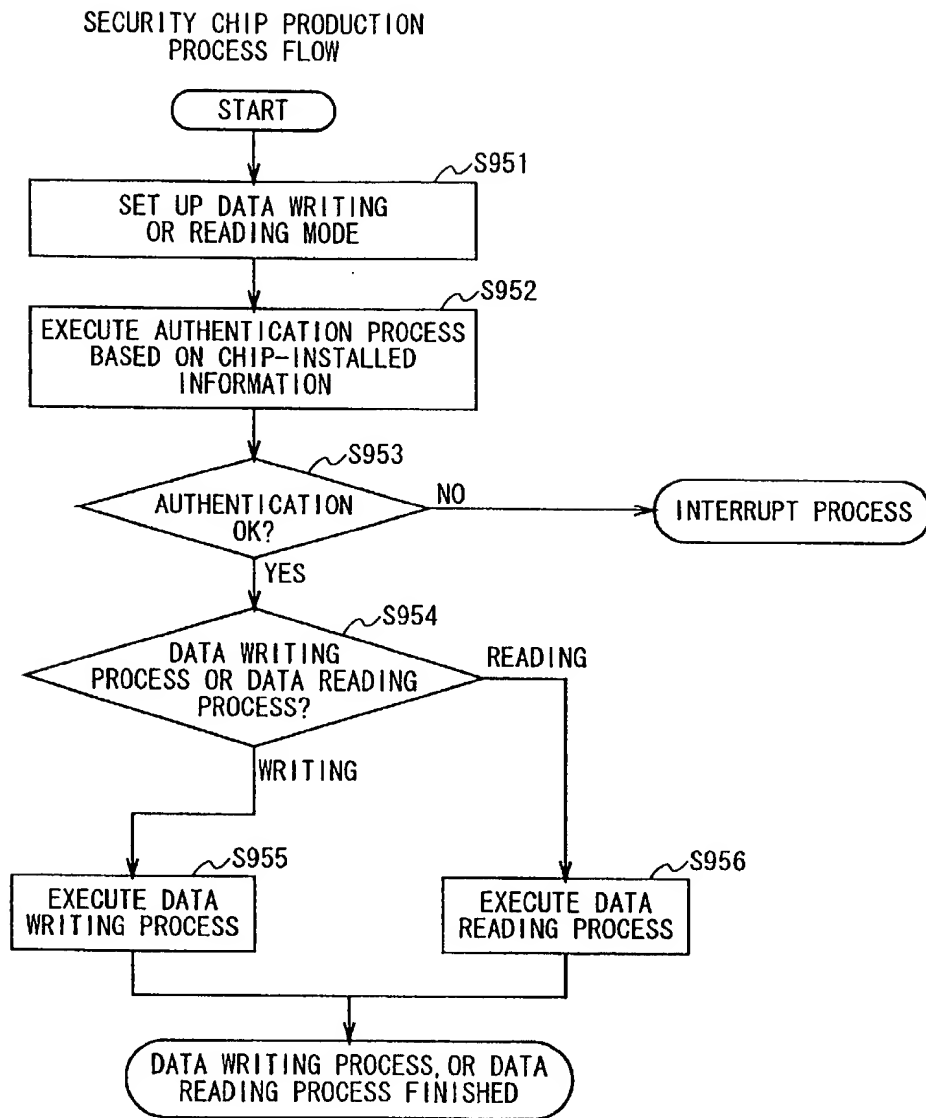
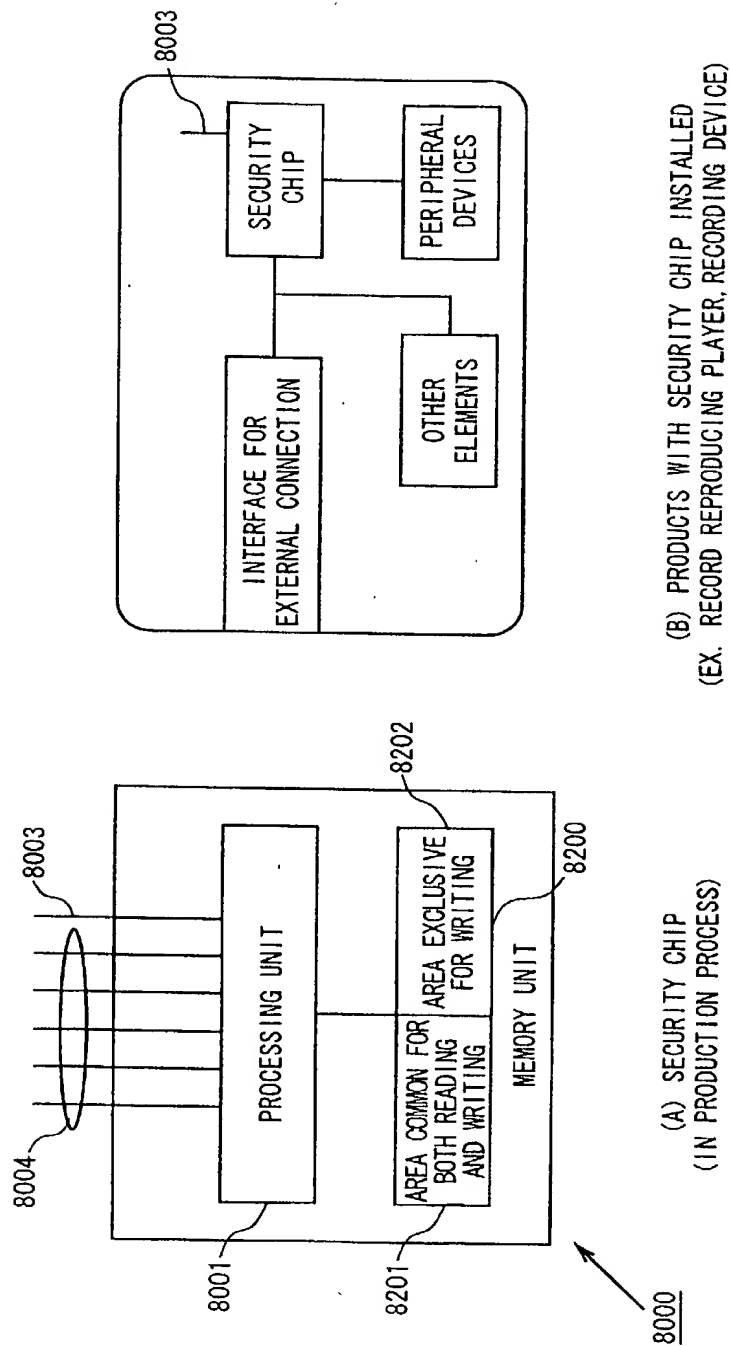
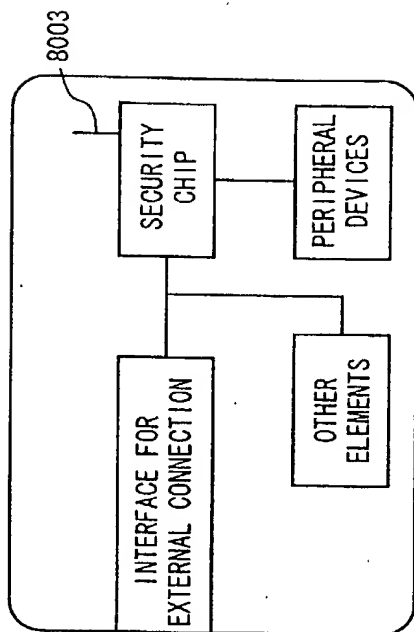


FIG. 90



(A) SECURITY CHIP  
(IN PRODUCTION PROCESS)



(B) PRODUCTS WITH SECURITY CHIP INSTALLED  
(EX. RECORD REPRODUCING PLAYER, RECORDING DEVICE)

FIG. 91

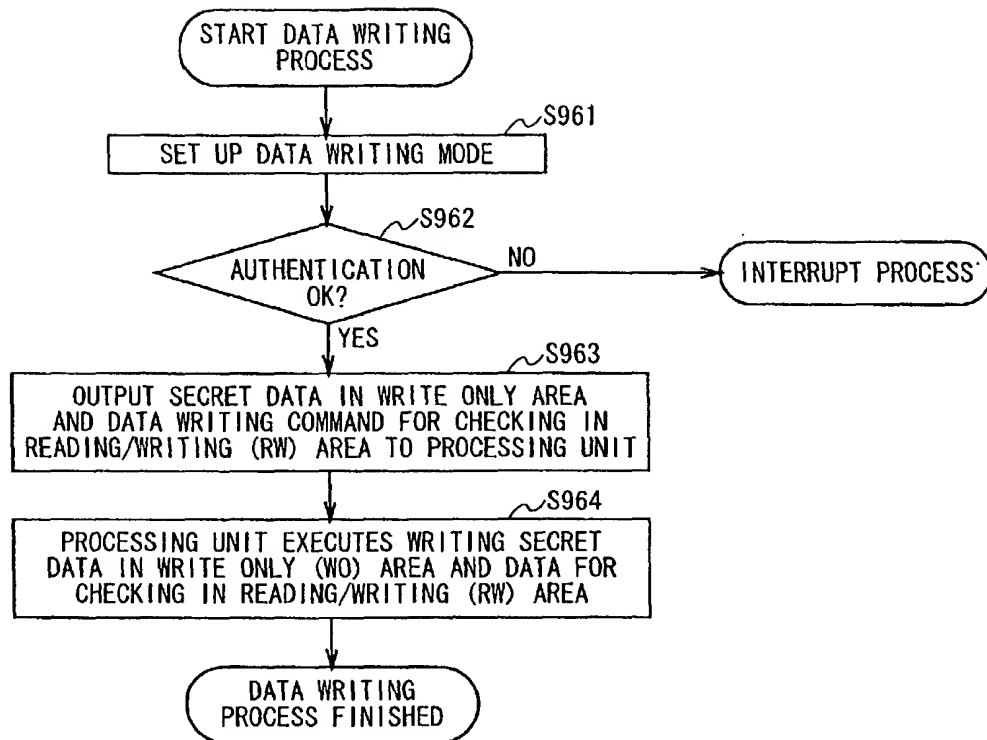


FIG. 92

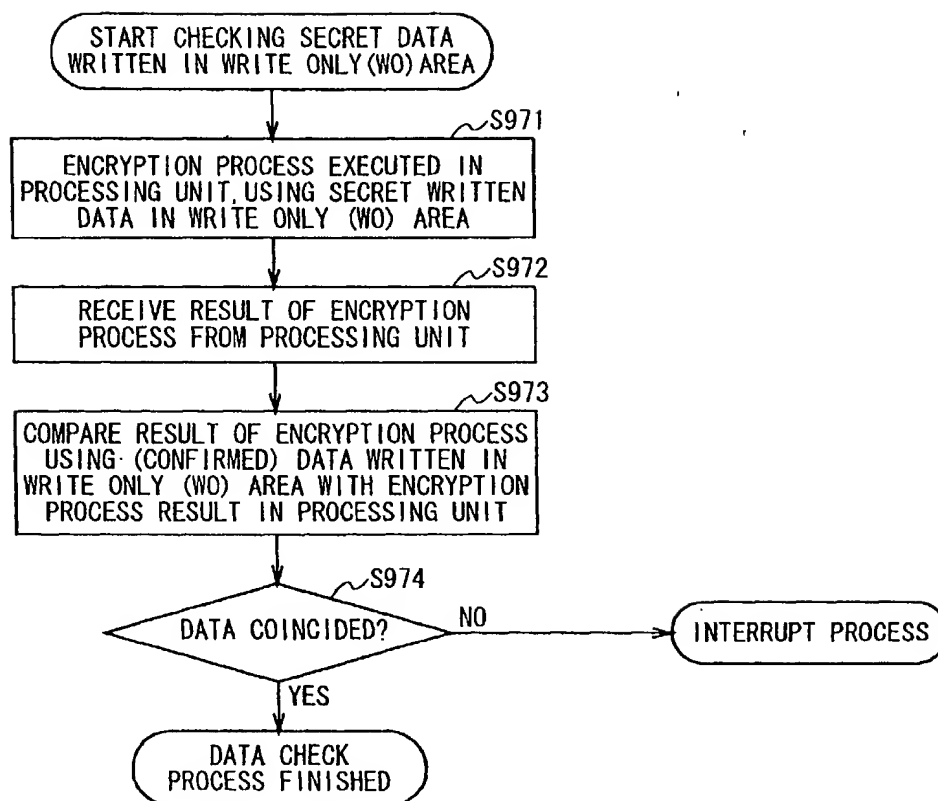


FIG. 93

## Explanation of Reference Numerals

106 - - main CPU, 107 - - RAM, 108 - - ROM, 109 - - AV processing unit, 110 - - input processing unit, 111 - - PIO, 112 - - SIO, 300 - - record reproduction player, 301 - - control unit, 302 - - encryption processing unit, 303 - - recording device controller, 304 - - read unit, 305 - - communication unit, 306 - - control unit, 307 - - internal memory, 308 - - encryption/decryption unit, 400 - - recording device, 401 - - encryption processing unit, 402 - - external memory, 403 - - control unit, 404 - - communication unit, 405 - - internal memory, 406 - - encryption/decryption unit, 407 - - external memory control unit, 500 - - media, 600 - - communication means, 2101, 2102, 2103 - - record reproduction player, 2104, 2105, 2106 - - recording device, 2901 - - command numbers management unit, 2902 - - command register, 2903, 2904 - - authentication flag, 3001 - - speaker, 3002 - - monitor, 3090 - - memory, 3091 - - contents analyzing unit, 3092 - - data memory unit, 3093 - program memory unit, 3094 - - compression/decompression processing unit, 7701 - - contents data, 7702 - revocation list, 7703 - - list check value, 8000 - - security chip, 8001 - - processing unit, 8002 - - memory unit, 8003 - - mode signal line, 8004 - - command signal line, 8201 - - read/write area, 8201 - write only area